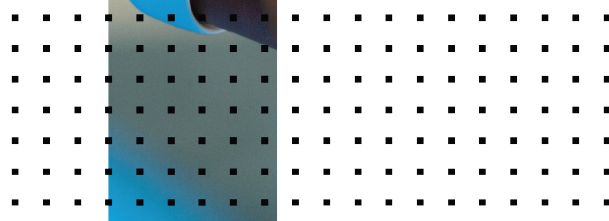
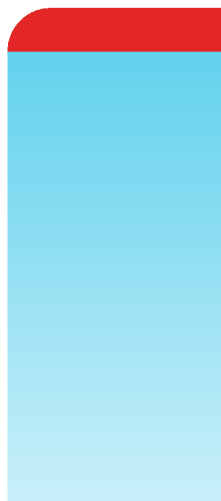


# CLI Reference

FortiOS 7.0.13



**FORTINET DOCUMENT LIBRARY**

<https://docs.fortinet.com>

**FORTINET VIDEO LIBRARY**

<https://video.fortinet.com>

**FORTINET BLOG**

<https://blog.fortinet.com>

**CUSTOMER SERVICE & SUPPORT**

<https://support.fortinet.com>

**FORTINET TRAINING & CERTIFICATION PROGRAM**

<https://www.fortinet.com/training-certification>

**FORTINET TRAINING INSTITUTE**

<https://training.fortinet.com>

**FORTIGUARD LABS**

<https://www.fortiguard.com>

**END USER LICENSE AGREEMENT**

<https://www.fortinet.com/doc/legal/EULA.pdf>

**FEEDBACK**

Email: [techdoc@fortinet.com](mailto:techdoc@fortinet.com)



October 26, 2023

FortiOS 7.0.13 CLI Reference

01-7013-709094-20231026

# TABLE OF CONTENTS

<b>Change Log</b>	<b>16</b>
<b>FortiOS CLI reference</b>	<b>17</b>
Availability of commands and options	17
Command tree	17
<b>CLI configuration commands</b>	<b>19</b>
alertemail	20
config alertemail setting	20
antivirus	27
config antivirus profile	27
config antivirus quarantine	55
config antivirus settings	60
application	62
config application custom	62
config application group	63
config application list	64
config application name	73
config application rule-settings	75
authentication	76
config authentication rule	76
config authentication scheme	78
config authentication setting	80
certificate	83
config certificate ca	83
config certificate crl	84
config certificate local	86
config certificate remote	89
dlp	91
config dlp filepattern	91
config dlp fp-doc-source	94
config dlp sensitivity	97
config dlp sensor	98
config dlp settings	103
dnsfilter	105
config dnsfilter domain-filter	105
config dnsfilter profile	106
dpdk	112
config dpdk cpus	112
config dpdk global	113
emailfilter	116
config emailfilter block-allow-list	116
config emailfilter bword	118
config emailfilter dnsbl	120
config emailfilter fortishield	121
config emailfilter iptrust	122

config emailfilter mheader .....	123
config emailfilter options .....	125
config emailfilter profile .....	125
endpoint-control .....	134
config endpoint-control fctems .....	134
extender-controller .....	139
config extender-controller dataplan .....	139
config extender-controller extender-profile .....	142
config extender-controller extender .....	153
file-filter .....	158
config file-filter profile .....	158
firewall .....	161
config firewall DoS-policy .....	163
config firewall DoS-policy6 .....	165
config firewall access-proxy-ssh-client-cert .....	168
config firewall access-proxy-virtual-host .....	170
config firewall access-proxy .....	171
config firewall access-proxy6 .....	192
config firewall acl .....	213
config firewall acl6 .....	214
config firewall address .....	215
config firewall address6-template .....	221
config firewall address6 .....	222
config firewall addgrp .....	226
config firewall addgrp6 .....	228
config firewall auth-portal .....	229
config firewall central-snat-map .....	230
config firewall city .....	232
config firewall country .....	233
config firewall decrypted-traffic-mirror .....	233
config firewall dnstranslation .....	234
config firewall gtp .....	236
config firewall identity-based-route .....	269
config firewall interface-policy .....	270
config firewall interface-policy6 .....	273
config firewall internet-service-addition .....	276
config firewall internet-service-append .....	277
config firewall internet-service-botnet .....	278
config firewall internet-service-custom-group .....	278
config firewall internet-service-custom .....	279
config firewall internet-service-definition .....	280
config firewall internet-service-extension .....	282
config firewall internet-service-group .....	285
config firewall internet-service-ipbl-reason .....	286
config firewall internet-service-ipbl-vendor .....	286
config firewall internet-service-list .....	287
config firewall internet-service-name .....	287
config firewall internet-service-owner .....	288
config firewall internet-service-reputation .....	289



config firewall internet-service-sld .....	289
config firewall internet-service .....	290
config firewall ip-translation .....	292
config firewall ipmacbinding setting .....	292
config firewall ipmacbinding table .....	293
config firewall ippool .....	294
config firewall ippool6 .....	298
config firewall ippool_grp .....	300
config firewall ipv6-eh-filter .....	301
config firewall ldb-monitor .....	302
config firewall local-in-policy .....	304
config firewall local-in-policy6 .....	306
config firewall multicast-address .....	308
config firewall multicast-address6 .....	310
config firewall multicast-policy .....	311
config firewall multicast-policy6 .....	313
config firewall pfcp .....	315
config firewall policy .....	318
config firewall profile-group .....	338
config firewall profile-protocol-options .....	340
config firewall proxy-address .....	364
config firewall proxy-addrgrp .....	368
config firewall proxy-policy .....	369
config firewall region .....	377
config firewall schedule group .....	377
config firewall schedule onetime .....	378
config firewall schedule recurring .....	379
config firewall security-policy .....	380
config firewall service category .....	388
config firewall service custom .....	388
config firewall service group .....	393
config firewall shaper per-ip-shaper .....	394
config firewall shaper traffic-shaper .....	395
config firewall shaping-policy .....	398
config firewall shaping-profile .....	402
config firewall sniffer .....	405
config firewall ssh host-key .....	410
config firewall ssh local-ca .....	412
config firewall ssh local-key .....	413
config firewall ssh setting .....	414
config firewall ssl-server .....	415
config firewall ssl-ssh-profile .....	417
config firewall ssl setting .....	446
config firewall traffic-class .....	448
config firewall ttl-policy .....	448
config firewall vendor-mac .....	449
config firewall vip .....	450
config firewall vip6 .....	481
config firewall vipgrp .....	510

config firewall vipgrp6 .....	511
config firewall wildcard-fqdn custom .....	512
config firewall wildcard-fqdn group .....	513
ftp-proxy .....	514
config ftp-proxy explicit .....	514
gtp .....	516
config gtp apn-shaper .....	516
config gtp apn .....	518
config gtp apngrp .....	519
config gtp ie-allow-list .....	520
config gtp message-filter-v0v1 .....	521
config gtp message-filter-v2 .....	529
config gtp rat-timeout-profile .....	534
config gtp tunnel-limit .....	536
icap .....	538
config icap profile .....	538
config icap server .....	543
ips .....	545
config ips custom .....	545
config ips decoder .....	547
config ips global .....	547
config ips rule-settings .....	551
config ips rule .....	551
config ips sensor .....	554
config ips settings .....	558
config ips view-map .....	559
log .....	561
config log custom-field .....	562
config log disk filter .....	563
config log disk setting .....	566
config log eventfilter .....	571
config log fortianalyzer-cloud filter .....	574
config log fortianalyzer-cloud override-filter .....	578
config log fortianalyzer-cloud override-setting .....	581
config log fortianalyzer-cloud setting .....	581
config log fortianalyzer2 filter .....	585
config log fortianalyzer2 override-filter .....	588
config log fortianalyzer2 override-setting .....	592
config log fortianalyzer2 setting .....	596
config log fortianalyzer3 filter .....	600
config log fortianalyzer3 override-filter .....	603
config log fortianalyzer3 override-setting .....	607
config log fortianalyzer3 setting .....	611
config log fortianalyzer filter .....	615
config log fortianalyzer override-filter .....	618
config log fortianalyzer override-setting .....	621
config log fortianalyzer setting .....	625
config log fortiguard filter .....	629
config log fortiguard override-filter .....	632

config log fortiguard override-setting .....	636
config log fortiguard setting .....	637
config log gui-display .....	640
config log memory filter .....	641
config log memory global-setting .....	644
config log memory setting .....	645
config log npu-server .....	645
config log null-device filter .....	649
config log null-device setting .....	652
config log setting .....	653
config log syslogd2 filter .....	657
config log syslogd2 override-filter .....	660
config log syslogd2 override-setting .....	664
config log syslogd2 setting .....	667
config log syslogd3 filter .....	671
config log syslogd3 override-filter .....	674
config log syslogd3 override-setting .....	678
config log syslogd3 setting .....	681
config log syslogd4 filter .....	685
config log syslogd4 override-filter .....	688
config log syslogd4 override-setting .....	692
config log syslogd4 setting .....	695
config log syslogd filter .....	699
config log syslogd override-filter .....	702
config log syslogd override-setting .....	706
config log syslogd setting .....	709
config log tacacs+accounting2 filter .....	713
config log tacacs+accounting2 setting .....	714
config log tacacs+accounting3 filter .....	714
config log tacacs+accounting3 setting .....	715
config log tacacs+accounting filter .....	716
config log tacacs+accounting setting .....	717
config log threat-weight .....	717
config log webtrends filter .....	728
config log webtrends setting .....	731
monitoring .....	732
config monitoring np6-ipsec-engine .....	732
config monitoring npu-hpe .....	733
nsxt .....	735
config nsxt service-chain .....	735
config nsxt setting .....	737
pfcp .....	738
config pfcp message-filter .....	738
report .....	742
config report layout .....	742
config report setting .....	751
router .....	753
config router access-list .....	753
config router access-list6 .....	754

config router aspath-list .....	756
config router auth-path .....	757
config router bfd .....	757
config router bfd6 .....	759
config router bgp .....	760
config router community-list .....	802
config router isis .....	803
config router key-chain .....	817
config router multicast-flow .....	818
config router multicast .....	819
config router multicast6 .....	828
config router ospf .....	830
config router ospf6 .....	846
config router policy .....	861
config router policy6 .....	864
config router prefix-list .....	866
config router prefix-list6 .....	867
config router rip .....	868
config router ripng .....	875
config router route-map .....	881
config router setting .....	887
config router static .....	887
config router static6 .....	890
sctp-filter .....	893
config sctp-filter profile .....	893
ssh-filter .....	895
config ssh-filter profile .....	895
switch-controller .....	898
config switch-controller 802-1X-settings .....	899
config switch-controller auto-config custom .....	901
config switch-controller auto-config default .....	902
config switch-controller auto-config policy .....	903
config switch-controller custom-command .....	905
config switch-controller dsl policy .....	906
config switch-controller dynamic-port-policy .....	909
config switch-controller flow-tracking .....	912
config switch-controller fortilink-settings .....	915
config switch-controller global .....	917
config switch-controller igmp-snooping .....	921
config switch-controller initial-config template .....	923
config switch-controller initial-config vlans .....	925
config switch-controller lldp-profile .....	926
config switch-controller lldp-settings .....	930
config switch-controller location .....	932
config switch-controller mac-policy .....	937
config switch-controller managed-switch .....	939
config switch-controller network-monitor-settings .....	974
config switch-controller ptp policy .....	975
config switch-controller ptp settings .....	976

config switch-controller qos dot1p-map .....	977
config switch-controller qos ip-dscp-map .....	981
config switch-controller qos qos-policy .....	984
config switch-controller qos queue-policy .....	985
config switch-controller quarantine .....	988
config switch-controller remote-log .....	989
config switch-controller security-policy 802-1X .....	992
config switch-controller security-policy local-access .....	995
config switch-controller sflow .....	997
config switch-controller snmp-community .....	998
config switch-controller snmp-sysinfo .....	1001
config switch-controller snmp-trap-threshold .....	1002
config switch-controller snmp-user .....	1004
config switch-controller storm-control-policy .....	1006
config switch-controller storm-control .....	1008
config switch-controller stp-instance .....	1010
config switch-controller stp-settings .....	1011
config switch-controller switch-group .....	1013
config switch-controller switch-interface-tag .....	1014
config switch-controller switch-log .....	1015
config switch-controller switch-profile .....	1016
config switch-controller system .....	1018
config switch-controller traffic-policy .....	1020
config switch-controller traffic-sniffer .....	1022
config switch-controller virtual-port-pool .....	1024
config switch-controller vlan-policy .....	1025
system .....	1027
config system 3g-modem custom .....	1030
config system accprofile .....	1031
config system acme .....	1041
config system admin .....	1042
config system affinity-interrupt .....	1049
config system affinity-packet-redistribution .....	1050
config system alarm .....	1051
config system alias .....	1054
config system api-user .....	1055
config system arp-table .....	1056
config system auto-install .....	1057
config system auto-script .....	1058
config system automation-action .....	1059
config system automation-destination .....	1064
config system automation-stitch .....	1064
config system automation-trigger .....	1066
config system autoupdate schedule .....	1070
config system autoupdate tunneling .....	1071
config system bypass .....	1072
config system central-management .....	1073
config system cluster-sync .....	1078
config system console .....	1081

config system csf .....	1082
config system custom-language .....	1087
config system ddns .....	1088
config system dedicated-mgmt .....	1090
config system dhcp6 server .....	1091
config system dhcp server .....	1095
config system dnp3-proxy .....	1107
config system dns-database .....	1109
config system dns-server .....	1112
config system dns .....	1113
config system dns64 .....	1116
config system dscp-based-priority .....	1116
config system elbc .....	1117
config system email-server .....	1118
config system external-resource .....	1120
config system federated-upgrade .....	1123
config system fips-cc .....	1125
config system fortiguard .....	1126
config system fortindr .....	1134
config system fortisandbox .....	1135
config system fsso-polling .....	1137
config system ftm-push .....	1138
config system geneve .....	1138
config system geoip-override .....	1139
config system gi-gk .....	1141
config system global .....	1142
config system gre-tunnel .....	1193
config system ha-monitor .....	1196
config system ha .....	1197
config system ike .....	1210
config system interface .....	1223
config system ipam .....	1282
config system ipip-tunnel .....	1283
config system ips-urlfilter-dns .....	1284
config system ips-urlfilter-dns6 .....	1285
config system ips .....	1285
config system ipsec-aggregate .....	1286
config system ipv6-neighbor-cache .....	1287
config system ipv6-tunnel .....	1287
config system isf-queue-profile .....	1289
config system link-monitor .....	1291
config system lldp network-policy .....	1296
config system lte-modem .....	1304
config system mac-address-table .....	1309
config system management-tunnel .....	1309
config system mobile-tunnel .....	1311
config system modem .....	1314
config system nd-proxy .....	1321
config system netflow .....	1322

config system network-visibility .....	1323
config system np6 .....	1325
config system np6xlite .....	1337
config system npu-setting prp .....	1350
config system npu-vlink .....	1351
config system npu .....	1352
config system ntp .....	1411
config system object-tagging .....	1414
config system password-policy-guest-admin .....	1415
config system password-policy .....	1417
config system physical-switch .....	1419
config system pppoe-interface .....	1420
config system probe-response .....	1422
config system proxy-arp .....	1424
config system ptp .....	1424
config system replacemsg-group .....	1426
config system replacemsg-image .....	1438
config system replacemsg admin .....	1439
config system replacemsg alertmail .....	1440
config system replacemsg auth .....	1441
config system replacemsg automation .....	1442
config system replacemsg custom-message .....	1443
config system replacemsg fortiguard-wf .....	1443
config system replacemsg ftp .....	1444
config system replacemsg http .....	1445
config system replacemsg icap .....	1446
config system replacemsg mail .....	1447
config system replacemsg nac-quar .....	1448
config system replacemsg spam .....	1449
config system replacemsg sslvpn .....	1449
config system replacemsg traffic-quota .....	1450
config system replacemsg utm .....	1451
config system replacemsg webproxy .....	1452
config system resource-limits .....	1453
config system saml .....	1456
config system sdn-connector .....	1459
config system sdwan .....	1468
config system session-helper .....	1488
config system session-ttl .....	1490
config system settings .....	1491
config system sflow .....	1513
config system sit-tunnel .....	1514
config system smc-ntp .....	1516
config system sms-server .....	1517
config system snmp community .....	1518
config system snmp sysinfo .....	1525
config system snmp user .....	1527
config system speed-test-schedule .....	1533
config system speed-test-server .....	1535

config system sso-admin .....	1536
config system sso-forticloud-admin .....	1537
config system standalone-cluster .....	1537
config system storage .....	1538
config system stp .....	1540
config system switch-interface .....	1542
config system tos-based-priority .....	1544
config system vdom-dns .....	1545
config system vdom-exception .....	1546
config system vdom-link .....	1548
config system vdom-netflow .....	1549
config system vdom-property .....	1550
config system vdom-radius-server .....	1552
config system vdom-sflow .....	1552
config system vdom .....	1553
config system virtual-switch .....	1555
config system virtual-wire-pair .....	1557
config system vne-tunnel .....	1558
config system vxlan .....	1559
config system wccp .....	1560
config system wireless ap-status .....	1564
config system wireless settings .....	1565
config system zone .....	1568
user .....	1570
config user adgrp .....	1570
config user certificate .....	1571
config user domain-controller .....	1572
config user exchange .....	1575
config user fortitoken .....	1577
config user fsso-polling .....	1578
config user fsso .....	1580
config user group .....	1584
config user krb-keytab .....	1589
config user ldap .....	1590
config user local .....	1596
config user nac-policy .....	1599
config user password-policy .....	1601
config user peer .....	1602
config user peergrp .....	1604
config user pop3 .....	1604
config user quarantine .....	1605
config user radius .....	1607
config user saml .....	1618
config user security-exempt-list .....	1622
config user setting .....	1623
config user tacacs+ .....	1627
videofilter .....	1630
config videofilter profile .....	1630
config videofilter youtube-channel-filter .....	1632



config videofilter youtube-key .....	1634
voip .....	1635
config voip profile .....	1635
vpn .....	1660
config vpn certificate ca .....	1660
config vpn certificate crt .....	1662
config vpn certificate local .....	1663
config vpn certificate ocsdp-server .....	1667
config vpn certificate remote .....	1668
config vpn certificate setting .....	1668
config vpn ipsec concentrator .....	1673
config vpn ipsec fec .....	1674
config vpn ipsec forticlient .....	1676
config vpn ipsec manualkey-interface .....	1676
config vpn ipsec manualkey .....	1679
config vpn ipsec phase1-interface .....	1681
config vpn ipsec phase1 .....	1706
config vpn ipsec phase2-interface .....	1725
config vpn ipsec phase2 .....	1735
config vpn l2tp .....	1744
config vpn ocvpn .....	1745
config vpn pptp .....	1749
config vpn ssl client .....	1750
config vpn ssl settings .....	1752
config vpn ssl web host-check-software .....	1765
config vpn ssl web portal .....	1767
config vpn ssl web realm .....	1786
config vpn ssl web user-bookmark .....	1787
config vpn ssl web user-group-bookmark .....	1794
waf .....	1801
config waf main-class .....	1801
config waf profile .....	1801
config waf signature .....	1826
config waf sub-class .....	1827
wanopt .....	1828
config wanopt auth-group .....	1828
config wanopt cache-service .....	1830
config wanopt content-delivery-network-rule .....	1833
config wanopt peer .....	1839
config wanopt profile .....	1840
config wanopt remote-storage .....	1849
config wanopt settings .....	1850
config wanopt webcache .....	1852
web-proxy .....	1856
config web-proxy debug-url .....	1856
config web-proxy explicit .....	1857
config web-proxy forward-server-group .....	1862
config web-proxy forward-server .....	1863
config web-proxy global .....	1865

config web-proxy profile .....	1867
config web-proxy url-match .....	1872
config web-proxy wisp .....	1872
webfilter .....	1874
config webfilter content-header .....	1874
config webfilter content .....	1875
config webfilter fortiguard .....	1877
config webfilter ftgd-local-cat .....	1879
config webfilter ftgd-local-rating .....	1880
config webfilter ips-urlfilter-cache-setting .....	1881
config webfilter ips-urlfilter-setting .....	1881
config webfilter ips-urlfilter-setting6 .....	1882
config webfilter override .....	1882
config webfilter profile .....	1884
config webfilter search-engine .....	1901
config webfilter urlfilter .....	1903
wireless-controller .....	1906
config wireless-controller access-control-list .....	1907
config wireless-controller address .....	1909
config wireless-controller addrgrp .....	1910
config wireless-controller ap-status .....	1911
config wireless-controller apcfg-profile .....	1911
config wireless-controller arrp-profile .....	1913
config wireless-controller ble-profile .....	1916
config wireless-controller bonjour-profile .....	1918
config wireless-controller global .....	1920
config wireless-controller hotspot20 anqp-3gpp-cellular .....	1923
config wireless-controller hotspot20 anqp-ip-address-type .....	1924
config wireless-controller hotspot20 anqp-nai-realm .....	1925
config wireless-controller hotspot20 anqp-network-auth-type .....	1929
config wireless-controller hotspot20 anqp-roaming-consortium .....	1929
config wireless-controller hotspot20 anqp-venue-name .....	1930
config wireless-controller hotspot20 anqp-venue-url .....	1931
config wireless-controller hotspot20 h2qp-advice-of-charge .....	1932
config wireless-controller hotspot20 h2qp-conn-capability .....	1933
config wireless-controller hotspot20 h2qp-operator-name .....	1936
config wireless-controller hotspot20 h2qp-osu-provider-nai .....	1937
config wireless-controller hotspot20 h2qp-osu-provider .....	1938
config wireless-controller hotspot20 h2qp-terms-and-conditions .....	1939
config wireless-controller hotspot20 h2qp-wan-metric .....	1940
config wireless-controller hotspot20 hs-profile .....	1941
config wireless-controller hotspot20 icon .....	1949
config wireless-controller hotspot20 qos-map .....	1950
config wireless-controller inter-controller .....	1952
config wireless-controller log .....	1954
config wireless-controller mpsk-profile .....	1958
config wireless-controller nac-profile .....	1960
config wireless-controller qos-profile .....	1961
config wireless-controller region .....	1964

---

config wireless-controller setting .....	1965
config wireless-controller snmp .....	1974
config wireless-controller ssid-policy .....	1978
config wireless-controller syslog-profile .....	1979
config wireless-controller timers .....	1980
config wireless-controller vap-group .....	1982
config wireless-controller vap .....	1983
config wireless-controller wag-profile .....	2015
config wireless-controller wids-profile .....	2017
config wireless-controller wtp-group .....	2024
config wireless-controller wtp-profile .....	2027
config wireless-controller wtp .....	2099

## Change Log

Date	Change Description
2023-10-26	First automated release of the FortiOS 7.0.13 CLI Reference.

# FortiOS CLI reference

This document describes FortiOS 7.0.13 CLI commands used to configure and manage a FortiGate unit from the command line interface (CLI). For information on using the CLI, see the [FortiOS 7.0.13 Administration Guide](#), which contains information such as:

- [Connecting to the CLI](#)
- [CLI basics](#)
- [Command syntax](#)
- [Subcommands](#)
- [Permissions](#)

## Availability of commands and options

Some FortiOS CLI commands and options are not available on all FortiGate units. The CLI displays an error message if you attempt to enter a command or option that is not available. You can use the question mark '?' to verify the commands and options that are available.

Commands and options may not be available for the following reasons:

### FortiGate model

All commands are not available on all FortiGate models. For example, a hardware switch can be configured only on models which have the corresponding hardware switch chipset.

### Hardware configuration

For example, settings like `mediatype` would only be available on units with SFPs.

### FortiOS Carrier, FortiGate 5K/6K/7K, FortiGate with LTE, etc.

Commands for extended functionality are not available on all FortiGate models. The CLI Reference may not include all commands.

## Command tree

Enter `tree` to display the entire FortiOS CLI command tree. To capture the full output, connect to your device using a terminal emulation program, such as PuTTY, and capture the output to a log file.

- To view all available commands, enter `tree`.
- To view a specific configuration branch of a tree, enter `tree <branch>`, for example: `tree system`.

- To view all available `diagnose` commands, enter `tree diagnose`.
- To view all available `execute` commands, enter `tree execute`.

# CLI configuration commands

Use configuration commands to configure and manage a FortiGate unit from the command line interface (CLI).

The CLI syntax is created by processing the schema from FortiGate models running FortiOS 7.0.13 and reformatting the resultant CLI output.

If you have comments on this content, its format, or requests for commands that are not included, contact us at [techdoc@fortinet.com](mailto:techdoc@fortinet.com).

## alertemail

This section includes syntax for the following commands:

- [config alertemail setting on page 20](#)

### config alertemail setting

Configure alert email settings.

```
config alertemail setting
    Description: Configure alert email settings.
    set FDS-license-expiring-days {integer}
    set FDS-license-expiring-warning [enable|disable]
    set FDS-update-logs [enable|disable]
    set FIPS-CC-errors [enable|disable]
    set FSSO-disconnect-logs [enable|disable]
    set HA-logs [enable|disable]
    set IPS-logs [enable|disable]
    set IPsec-errors-logs [enable|disable]
    set PPP-errors-logs [enable|disable]
    set admin-login-logs [enable|disable]
    set alert-interval {integer}
    set amc-interface-bypass-mode [enable|disable]
    set antivirus-logs [enable|disable]
    set configuration-changes-logs [enable|disable]
    set critical-interval {integer}
    set debug-interval {integer}
    set email-interval {integer}
    set emergency-interval {integer}
    set error-interval {integer}
    set filter-mode [category|threshold]
    set firewall-authentication-failure-logs [enable|disable]
    set fortiguard-log-quota-warning [enable|disable]
    set information-interval {integer}
    set local-disk-usage {integer}
    set log-disk-usage-warning [enable|disable]
    set mailto1 {string}
    set mailto2 {string}
    set mailto3 {string}
    set notification-interval {integer}
    set severity [emergency|alert|...]
    set ssh-logs [enable|disable]
    set sslvpn-authentication-errors-logs [enable|disable]
    set username {string}
    set violation-traffic-logs [enable|disable]
    set warning-interval {integer}
    set webfilter-logs [enable|disable]
end
```



## config alertemail setting

Parameter	Description	Type	Size	Default						
FDS-license-expiring-days	Number of days to send alert email prior to FortiGuard license expiration.	integer	Minimum value: 1 Maximum value: 100	15						
FDS-license-expiring-warning	Enable/disable FortiGuard license expiration warnings in alert email.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable FortiGuard license expiration warnings in alert email.</td></tr><tr><td><i>disable</i></td><td>Disable FortiGuard license expiration warnings in alert email.</td></tr></table>	Option	Description	<i>enable</i>	Enable FortiGuard license expiration warnings in alert email.	<i>disable</i>	Disable FortiGuard license expiration warnings in alert email.			
Option	Description									
<i>enable</i>	Enable FortiGuard license expiration warnings in alert email.									
<i>disable</i>	Disable FortiGuard license expiration warnings in alert email.									
FDS-update-logs	Enable/disable FortiGuard update logs in alert email.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable FortiGuard update logs in alert email.</td></tr><tr><td><i>disable</i></td><td>Disable FortiGuard update logs in alert email.</td></tr></table>	Option	Description	<i>enable</i>	Enable FortiGuard update logs in alert email.	<i>disable</i>	Disable FortiGuard update logs in alert email.			
Option	Description									
<i>enable</i>	Enable FortiGuard update logs in alert email.									
<i>disable</i>	Disable FortiGuard update logs in alert email.									
FIPS-CC-errors	Enable/disable FIPS and Common Criteria error logs in alert email.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable FIPS and Common Criteria error logs in alert email.</td></tr><tr><td><i>disable</i></td><td>Disable FIPS and Common Criteria error logs in alert email.</td></tr></table>	Option	Description	<i>enable</i>	Enable FIPS and Common Criteria error logs in alert email.	<i>disable</i>	Disable FIPS and Common Criteria error logs in alert email.			
Option	Description									
<i>enable</i>	Enable FIPS and Common Criteria error logs in alert email.									
<i>disable</i>	Disable FIPS and Common Criteria error logs in alert email.									
FSSO-disconnect-logs	Enable/disable logging of FSSO collector agent disconnect.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable logging of FSSO collector agent disconnect.</td></tr><tr><td><i>disable</i></td><td>Disable logging of FSSO collector agent disconnect.</td></tr></table>	Option	Description	<i>enable</i>	Enable logging of FSSO collector agent disconnect.	<i>disable</i>	Disable logging of FSSO collector agent disconnect.			
Option	Description									
<i>enable</i>	Enable logging of FSSO collector agent disconnect.									
<i>disable</i>	Disable logging of FSSO collector agent disconnect.									
HA-logs	Enable/disable HA logs in alert email.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable HA logs in alert email.</td></tr><tr><td><i>disable</i></td><td>Disable HA logs in alert email.</td></tr></table>	Option	Description	<i>enable</i>	Enable HA logs in alert email.	<i>disable</i>	Disable HA logs in alert email.			
Option	Description									
<i>enable</i>	Enable HA logs in alert email.									
<i>disable</i>	Disable HA logs in alert email.									
IPS-logs	Enable/disable IPS logs in alert email.	option	-	disable						

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable IPS logs in alert email.		
	<i>disable</i>	Disable IPS logs in alert email.		
IPsec-errors-logs	Enable/disable IPsec error logs in alert email.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable IPsec error logs in alert email.		
	<i>disable</i>	Disable IPsec error logs in alert email.		
PPP-errors-logs	Enable/disable PPP error logs in alert email.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable PPP error logs in alert email.		
	<i>disable</i>	Disable PPP error logs in alert email.		
admin-login-logs	Enable/disable administrator login/logout logs in alert email.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable administrator login/logout logs in alert email.		
	<i>disable</i>	Disable administrator login/logout logs in alert email.		
alert-interval	Alert alert interval in minutes.	integer	Minimum value: 1 Maximum value: 99999	2
amc-interface-bypass-mode	Enable/disable Fortinet Advanced Mezzanine Card (AMC) interface bypass mode logs in alert email.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable Fortinet Advanced Mezzanine Card (AMC) interface bypass mode logs in alert email.		
	<i>disable</i>	Disable Fortinet Advanced Mezzanine Card (AMC) interface bypass mode logs in alert email.		
antivirus-logs	Enable/disable antivirus logs in alert email.	option	-	disable

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable antivirus logs in alert email.</td></tr><tr><td><i>disable</i></td><td>Disable antivirus logs in alert email.</td></tr></table>	Option	Description	<i>enable</i>	Enable antivirus logs in alert email.	<i>disable</i>	Disable antivirus logs in alert email.			
	Option	Description								
	<i>enable</i>	Enable antivirus logs in alert email.								
<i>disable</i>	Disable antivirus logs in alert email.									
configuration-changes-logs	Enable/disable configuration change logs in alert email.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable configuration change logs in alert email.</td></tr><tr><td><i>disable</i></td><td>Disable configuration change logs in alert email.</td></tr></table>	Option	Description	<i>enable</i>	Enable configuration change logs in alert email.	<i>disable</i>	Disable configuration change logs in alert email.			
	Option	Description								
	<i>enable</i>	Enable configuration change logs in alert email.								
<i>disable</i>	Disable configuration change logs in alert email.									
critical-interval	Critical alert interval in minutes.	integer	Minimum value: 1 Maximum value: 99999	3						
debug-interval	Debug alert interval in minutes.	integer	Minimum value: 1 Maximum value: 99999	60						
email-interval	Interval between sending alert emails.	integer	Minimum value: 1 Maximum value: 99999	5						
emergency-interval	Emergency alert interval in minutes.	integer	Minimum value: 1 Maximum value: 99999	1						
error-interval	Error alert interval in minutes.	integer	Minimum value: 1 Maximum value: 99999	5						
filter-mode	How to filter log messages that are sent to alert emails.	option	-	category						

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>category</i></td><td>Filter based on category.</td></tr><tr><td><i>threshold</i></td><td>Filter based on severity.</td></tr></table>	Option	Description	<i>category</i>	Filter based on category.	<i>threshold</i>	Filter based on severity.			
	Option	Description								
	<i>category</i>	Filter based on category.								
<i>threshold</i>	Filter based on severity.									
firewall-authentication-failure-logs	Enable/disable firewall authentication failure logs in alert email.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable firewall authentication failure logs in alert email.</td></tr><tr><td><i>disable</i></td><td>Disable firewall authentication failure logs in alert email.</td></tr></table>	Option	Description	<i>enable</i>	Enable firewall authentication failure logs in alert email.	<i>disable</i>	Disable firewall authentication failure logs in alert email.			
	Option	Description								
	<i>enable</i>	Enable firewall authentication failure logs in alert email.								
<i>disable</i>	Disable firewall authentication failure logs in alert email.									
fortiguard-log-quota-warning	Enable/disable FortiCloud log quota warnings in alert email.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable FortiCloud log quota warnings in alert email.</td></tr><tr><td><i>disable</i></td><td>Disable FortiCloud log quota warnings in alert email.</td></tr></table>	Option	Description	<i>enable</i>	Enable FortiCloud log quota warnings in alert email.	<i>disable</i>	Disable FortiCloud log quota warnings in alert email.			
	Option	Description								
	<i>enable</i>	Enable FortiCloud log quota warnings in alert email.								
<i>disable</i>	Disable FortiCloud log quota warnings in alert email.									
information-interval	Information alert interval in minutes.	integer	Minimum value: 1 Maximum value: 99999	30						
local-disk-usage	Disk usage percentage at which to send alert email.	integer	Minimum value: 1 Maximum value: 99	75						
log-disk-usage-warning	Enable/disable disk usage warnings in alert email.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable disk usage warnings in alert email.</td></tr><tr><td><i>disable</i></td><td>Disable disk usage warnings in alert email.</td></tr></table>	Option	Description	<i>enable</i>	Enable disk usage warnings in alert email.	<i>disable</i>	Disable disk usage warnings in alert email.			
	Option	Description								
	<i>enable</i>	Enable disk usage warnings in alert email.								
<i>disable</i>	Disable disk usage warnings in alert email.									
mailto1	Email address to send alert email to (usually a system administrator) (max. 63 characters).	string	Maximum length: 63							
mailto2	Optional second email address to send alert email to (max. 63 characters).	string	Maximum length: 63							

Parameter	Description	Type	Size	Default																		
mailto3	Optional third email address to send alert email to (max. 63 characters).	string	Maximum length: 63																			
notification-interval	Notification alert interval in minutes.	integer	Minimum value: 1 Maximum value: 99999	20																		
severity	Lowest severity level to log.	option	-	alert																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>emergency</i></td><td>Emergency level.</td></tr><tr><td><i>alert</i></td><td>Alert level.</td></tr><tr><td><i>critical</i></td><td>Critical level.</td></tr><tr><td><i>error</i></td><td>Error level.</td></tr><tr><td><i>warning</i></td><td>Warning level.</td></tr><tr><td><i>notification</i></td><td>Notification level.</td></tr><tr><td><i>information</i></td><td>Information level.</td></tr><tr><td><i>debug</i></td><td>Debug level.</td></tr></table>				Option	Description	<i>emergency</i>	Emergency level.	<i>alert</i>	Alert level.	<i>critical</i>	Critical level.	<i>error</i>	Error level.	<i>warning</i>	Warning level.	<i>notification</i>	Notification level.	<i>information</i>	Information level.	<i>debug</i>	Debug level.
	Option	Description																				
	<i>emergency</i>	Emergency level.																				
	<i>alert</i>	Alert level.																				
	<i>critical</i>	Critical level.																				
	<i>error</i>	Error level.																				
	<i>warning</i>	Warning level.																				
	<i>notification</i>	Notification level.																				
	<i>information</i>	Information level.																				
<i>debug</i>	Debug level.																					
ssh-logs	Enable/disable SSH logs in alert email.	option	-	disable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable SSH logs in alert email.</td></tr><tr><td><i>disable</i></td><td>Disable SSH logs in alert email.</td></tr></table>				Option	Description	<i>enable</i>	Enable SSH logs in alert email.	<i>disable</i>	Disable SSH logs in alert email.												
	Option	Description																				
	<i>enable</i>	Enable SSH logs in alert email.																				
<i>disable</i>	Disable SSH logs in alert email.																					
sslvpn-authentication-errors-logs	Enable/disable SSL-VPN authentication error logs in alert email.	option	-	disable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable SSL-VPN authentication error logs in alert email.</td></tr><tr><td><i>disable</i></td><td>Disable SSL-VPN authentication error logs in alert email.</td></tr></table>				Option	Description	<i>enable</i>	Enable SSL-VPN authentication error logs in alert email.	<i>disable</i>	Disable SSL-VPN authentication error logs in alert email.												
	Option	Description																				
	<i>enable</i>	Enable SSL-VPN authentication error logs in alert email.																				
<i>disable</i>	Disable SSL-VPN authentication error logs in alert email.																					
username	Name that appears in the From: field of alert emails (max. 63 characters).	string	Maximum length: 63																			
violation-traffic-logs	Enable/disable violation traffic logs in alert email.	option	-	disable																		

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable violation traffic logs in alert email.		
	<i>disable</i>	Disable violation traffic logs in alert email.		
warning-interval	Warning alert interval in minutes.	integer	Minimum value: 1 Maximum value: 99999	10
webfilter-logs	Enable/disable web filter logs in alert email.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable web filter logs in alert email.		
	<i>disable</i>	Disable web filter logs in alert email.		

## antivirus

This section includes syntax for the following commands:

- [config antivirus profile on page 27](#)
- [config antivirus quarantine on page 55](#)
- [config antivirus settings on page 60](#)

### config antivirus profile

Configure AntiVirus profiles.

```
config antivirus profile
  Description: Configure AntiVirus profiles.
  edit <name>
    set analytics-accept-filetype {integer}
    set analytics-db [disable|enable]
    set analytics-ignore-filetype {integer}
    set analytics-max-upload {integer}
    set av-block-log [enable|disable]
    set av-virus-log [enable|disable]
  config cifs
    Description: Configure CIFS AntiVirus options.
    set av-scan [disable|block|...]
    set outbreak-prevention [disable|block|...]
    set external-blocklist [disable|block|...]
    set fortindr [disable|block|...]
    set quarantine [disable|enable]
    set archive-block {option1}, {option2}, ...
    set archive-log {option1}, {option2}, ...
    set emulator [enable|disable]
  end
  set comment {var-string}
config content-disarm
  Description: AV Content Disarm and Reconstruction settings.
  set original-file-destination [fortisandbox|quarantine|...]
  set error-action [block|log-only|...]
  set office-macro [disable|enable]
  set office-hylink [disable|enable]
  set office-linked [disable|enable]
  set office-embed [disable|enable]
  set office-dde [disable|enable]
  set office-action [disable|enable]
  set pdf-javacode [disable|enable]
  set pdf-embedfile [disable|enable]
  set pdf-hyperlink [disable|enable]
  set pdf-act-gotor [disable|enable]
  set pdf-act-launch [disable|enable]
  set pdf-act-sound [disable|enable]
  set pdf-act-movie [disable|enable]
```

```

        set pdf-act-java [disable|enable]
        set pdf-act-form [disable|enable]
        set cover-page [disable|enable]
        set detect-only [disable|enable]
    end
    set ems-threat-feed [disable|enable]
    set extended-log [enable|disable]
    set external-blocklist <name1>, <name2>, ...
    set external-blocklist-enable-all [disable|enable]
    set feature-set [flow|proxy]
    set fortindr-error-action [log-only|block|...]
    set fortindr-timeout-action [log-only|block|...]
    set ftgd-analytics [disable|suspicious|...]
    config ftp
        Description: Configure FTP AntiVirus options.
        set av-scan [disable|block|...]
        set outbreak-prevention [disable|block|...]
        set external-blocklist [disable|block|...]
        set fortindr [disable|block|...]
        set quarantine [disable|enable]
        set archive-block {option1}, {option2}, ...
        set archive-log {option1}, {option2}, ...
        set emulator [enable|disable]
    end
    config http
        Description: Configure HTTP AntiVirus options.
        set av-scan [disable|block|...]
        set outbreak-prevention [disable|block|...]
        set external-blocklist [disable|block|...]
        set fortindr [disable|block|...]
        set quarantine [disable|enable]
        set archive-block {option1}, {option2}, ...
        set archive-log {option1}, {option2}, ...
        set emulator [enable|disable]
        set unknown-content-encoding [block|inspect|...]
        set content-disarm [disable|enable]
    end
    config imap
        Description: Configure IMAP AntiVirus options.
        set av-scan [disable|block|...]
        set outbreak-prevention [disable|block|...]
        set external-blocklist [disable|block|...]
        set fortindr [disable|block|...]
        set quarantine [disable|enable]
        set archive-block {option1}, {option2}, ...
        set archive-log {option1}, {option2}, ...
        set emulator [enable|disable]
        set executables [default|virus]
        set content-disarm [disable|enable]
    end
    config mapi
        Description: Configure MAPI AntiVirus options.
        set av-scan [disable|block|...]
        set outbreak-prevention [disable|block|...]
        set external-blocklist [disable|block|...]
        set quarantine [disable|enable]

```



```

        set archive-block {option1}, {option2}, ...
        set archive-log {option1}, {option2}, ...
        set emulator [enable|disable]
        set executables [default|virus]
    end
    set mobile-malware-db [disable|enable]
    config nac-quar
        Description: Configure AntiVirus quarantine settings.
        set infected [none|quar-src-ip]
        set expiry {user}
        set log [enable|disable]
    end
    config nntp
        Description: Configure NNTP AntiVirus options.
        set av-scan [disable|block|...]
        set outbreak-prevention [disable|block|...]
        set external-blocklist [disable|block|...]
        set fortindr [disable|block|...]
        set quarantine [disable|enable]
        set archive-block {option1}, {option2}, ...
        set archive-log {option1}, {option2}, ...
        set emulator [enable|disable]
    end
    set outbreak-prevention-archive-scan [disable|enable]
    config pop3
        Description: Configure POP3 AntiVirus options.
        set av-scan [disable|block|...]
        set outbreak-prevention [disable|block|...]
        set external-blocklist [disable|block|...]
        set fortindr [disable|block|...]
        set quarantine [disable|enable]
        set archive-block {option1}, {option2}, ...
        set archive-log {option1}, {option2}, ...
        set emulator [enable|disable]
        set executables [default|virus]
        set content-disarm [disable|enable]
    end
    set replacemsg-group {string}
    set scan-mode [default|legacy]
    config smtp
        Description: Configure SMTP AntiVirus options.
        set av-scan [disable|block|...]
        set outbreak-prevention [disable|block|...]
        set external-blocklist [disable|block|...]
        set fortindr [disable|block|...]
        set quarantine [disable|enable]
        set archive-block {option1}, {option2}, ...
        set archive-log {option1}, {option2}, ...
        set emulator [enable|disable]
        set executables [default|virus]
        set content-disarm [disable|enable]
    end
    config ssh
        Description: Configure SFTP and SCP AntiVirus options.
        set av-scan [disable|block|...]
        set outbreak-prevention [disable|block|...]

```

```

        set external-blocklist [disable|block|...]
        set fortindr [disable|block|...]
        set quarantine [disable|enable]
        set archive-block {option1}, {option2}, ...
        set archive-log {option1}, {option2}, ...
        set emulator [enable|disable]
    end
next
end

```

## config antivirus profile

Parameter	Description	Type	Size	Default
analytics-accept-filetype	Only submit files matching this DLP file-pattern to FortiSandbox.	integer	Minimum value: 0 Maximum value: 4294967295	0
analytics-db	Enable/disable using the FortiSandbox signature database to supplement the AV signature databases.	option	-	disable
	Option	Description		
	disable	Use only the standard AV signature databases.		
	enable	Also use the FortiSandbox signature database.		
analytics-ignore-filetype	Do not submit files matching this DLP file-pattern to FortiSandbox.	integer	Minimum value: 0 Maximum value: 4294967295	0
analytics-max-upload	Maximum size of files that can be uploaded to FortiSandbox.	integer	Minimum value: 1 Maximum value: 1606 **	10
av-block-log	Enable/disable logging for AntiVirus file blocking.	option	-	enable
	Option	Description		
	enable	Enable setting.		
	disable	Disable setting.		
av-virus-log	Enable/disable AntiVirus logging.	option	-	enable

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
comment	Comment.	var-string	Maximum length: 255	
ems-threat-feed	Enable/disable use of EMS threat feed when performing AntiVirus scan. Analyzes files including the content of archives.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable use of EMS threat feed when performing AntiVirus scan.		
	<i>enable</i>	Enable use of EMS threat feed when performing AntiVirus scan.		
extended-log	Enable/disable extended logging for antivirus.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
external-blocklist <name>	One or more external malware block lists. External blocklist.	string	Maximum length: 79	
external-blocklist-enable-all	Enable/disable all external blocklists.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Use configured external blocklists.		
	<i>enable</i>	Enable all external blocklists.		
feature-set	Flow/proxy feature set.	option	-	flow
	<b>Option</b>	<b>Description</b>		
	<i>flow</i>	Flow feature set.		
	<i>proxy</i>	Proxy feature set.		
fortindr-error-action	Action to take if FortiNDR encounters an error.	option	-	log-only

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>log-only</td><td>Log FortiNDR error, but allow the file.</td></tr><tr><td>block</td><td>Block the file on FortiNDR error.</td></tr><tr><td>ignore</td><td>Do nothing on FortiNDR error.</td></tr></table>	Option	Description	log-only	Log FortiNDR error, but allow the file.	block	Block the file on FortiNDR error.	ignore	Do nothing on FortiNDR error.			
	Option	Description										
	log-only	Log FortiNDR error, but allow the file.										
	block	Block the file on FortiNDR error.										
ignore	Do nothing on FortiNDR error.											
fortindr-timeout-action	Action to take if FortiNDR encounters a scan timeout.	option	-	log-only								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>log-only</td><td>Log FortiNDR scan timeout, but allow the file.</td></tr><tr><td>block</td><td>Block the file on FortiNDR scan timeout.</td></tr><tr><td>ignore</td><td>Do nothing on FortiNDR scan timeout.</td></tr></table>	Option	Description	log-only	Log FortiNDR scan timeout, but allow the file.	block	Block the file on FortiNDR scan timeout.	ignore	Do nothing on FortiNDR scan timeout.			
	Option	Description										
	log-only	Log FortiNDR scan timeout, but allow the file.										
	block	Block the file on FortiNDR scan timeout.										
ignore	Do nothing on FortiNDR scan timeout.											
ftgd-analytics	Settings to control which files are uploaded to FortiSandbox.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Do not upload files to FortiSandbox.</td></tr><tr><td>suspicious</td><td>Submit files supported by FortiSandbox if heuristics or other methods determine they are suspicious.</td></tr><tr><td>everything</td><td>Submit files supported by FortiSandbox and known infected files.</td></tr></table>	Option	Description	disable	Do not upload files to FortiSandbox.	suspicious	Submit files supported by FortiSandbox if heuristics or other methods determine they are suspicious.	everything	Submit files supported by FortiSandbox and known infected files.			
	Option	Description										
	disable	Do not upload files to FortiSandbox.										
	suspicious	Submit files supported by FortiSandbox if heuristics or other methods determine they are suspicious.										
everything	Submit files supported by FortiSandbox and known infected files.											
mobile-malware-db	Enable/disable using the mobile malware signature database.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Do not use the mobile malware signature database.</td></tr><tr><td>enable</td><td>Also use the mobile malware signature database.</td></tr></table>	Option	Description	disable	Do not use the mobile malware signature database.	enable	Also use the mobile malware signature database.					
	Option	Description										
	disable	Do not use the mobile malware signature database.										
enable	Also use the mobile malware signature database.											
name	Profile name.	string	Maximum length: 35									
outbreak-prevention-archive-scan	Enable/disable outbreak-prevention archive scanning.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Analyze files as sent, not the content of archives.</td></tr><tr><td>enable</td><td>Analyze files including the content of archives.</td></tr></table>	Option	Description	disable	Analyze files as sent, not the content of archives.	enable	Analyze files including the content of archives.					
	Option	Description										
	disable	Analyze files as sent, not the content of archives.										
enable	Analyze files including the content of archives.											

Parameter	Description	Type	Size	Default
replacemsg-group	Replacement message group customized for this profile.	string	Maximum length: 35	
scan-mode	Configure scan mode.	option	-	default
	Option	Description		
	default	On the fly decompression and scanning of certain archive files.		
	legacy	Scan archive files only after the entire file is received.		

\*\* Values may differ between models.

## config cifs

Parameter	Description	Type	Size	Default
av-scan	Enable AntiVirus scan service.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable.		
	<i>block</i>	Block the virus infected files.		
	<i>monitor</i>	Log the virus infected files.		
outbreak-prevention	Enable virus outbreak prevention service.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable.		
	<i>block</i>	Block the matched files.		
	<i>monitor</i>	Log the matched files.		
external-blocklist	Enable external-blocklist. Analyzes files including the content of archives.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable.		
	<i>block</i>	Block the matched files.		
	<i>monitor</i>	Log the matched files.		
fortindr	Enable/disable scanning of files by FortiNDR.	option	-	disable

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable.		
	<i>block</i>	Block the FortiNDR detected infections.		
	<i>monitor</i>	Log the FortiNDR detected infections.		
quarantine	Enable/disable quarantine for infected files.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable quarantine for infected files.		
	<i>enable</i>	Enable quarantine for infected files.		
archive-block	Select the archive types to block.	option	-	
	<b>Option</b>	<b>Description</b>		
	<i>encrypted</i>	Block encrypted archives.		
	<i>corrupted</i>	Block corrupted archives.		
	<i>partiallycorrupted</i>	Block partially corrupted archives.		
	<i>multipart</i>	Block multipart archives.		
	<i>nested</i>	Block nested archives that exceed uncompressed nest limit.		
	<i>mailbomb</i>	Block mail bomb archives.		
	<i>timeout</i>	Block scan timeout.		
	<i>unhandled</i>	Block archives that FortiOS cannot open.		
archive-log	Select the archive types to log.	option	-	
	<b>Option</b>	<b>Description</b>		
	<i>encrypted</i>	Log encrypted archives.		
	<i>corrupted</i>	Log corrupted archives.		
	<i>partiallycorrupted</i>	Log partially corrupted archives.		
	<i>multipart</i>	Log multipart archives.		
	<i>nested</i>	Log nested archives that exceed uncompressed nest limit.		
	<i>mailbomb</i>	Log mail bomb archives.		
	<i>timeout</i>	Log scan timeout.		
	<i>unhandled</i>	Log archives that FortiOS cannot open.		
emulator	Enable/disable the virus emulator.	option	-	enable

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable the virus emulator.		
	<i>disable</i>	Disable the virus emulator.		

## config content-disarm

Parameter	Description	Type	Size	Default
original-file-destination	Destination to send original file if active content is removed.	option	-	discard
	<b>Option</b>	<b>Description</b>		
	<i>fortisandbox</i>	Send original file to configured FortiSandbox.		
	<i>quarantine</i>	Send original file to quarantine.		
	<i>discard</i>	Original file will be discarded after content disarm.		
error-action	Action to be taken if CDR engine encounters an unrecoverable error.	option	-	log-only
	<b>Option</b>	<b>Description</b>		
	<i>block</i>	Block file on CDR error.		
	<i>log-only</i>	Log CDR error, but allow file.		
	<i>ignore</i>	Do nothing on CDR error.		
office-macro	Enable/disable stripping of macros in Microsoft Office documents.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable this Content Disarm and Reconstruction feature.		
	<i>enable</i>	Enable this Content Disarm and Reconstruction feature.		
office-hylink	Enable/disable stripping of hyperlinks in Microsoft Office documents.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable this Content Disarm and Reconstruction feature.		
	<i>enable</i>	Enable this Content Disarm and Reconstruction feature.		
office-linked	Enable/disable stripping of linked objects in Microsoft Office documents.	option	-	enable

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable this Content Disarm and Reconstruction feature.		
	<i>enable</i>	Enable this Content Disarm and Reconstruction feature.		
office-embed	Enable/disable stripping of embedded objects in Microsoft Office documents.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable this Content Disarm and Reconstruction feature.		
	<i>enable</i>	Enable this Content Disarm and Reconstruction feature.		
office-dde	Enable/disable stripping of Dynamic Data Exchange events in Microsoft Office documents.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable this Content Disarm and Reconstruction feature.		
	<i>enable</i>	Enable this Content Disarm and Reconstruction feature.		
office-action	Enable/disable stripping of PowerPoint action events in Microsoft Office documents.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable this Content Disarm and Reconstruction feature.		
	<i>enable</i>	Enable this Content Disarm and Reconstruction feature.		
pdf-javacode	Enable/disable stripping of JavaScript code in PDF documents.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable this Content Disarm and Reconstruction feature.		
	<i>enable</i>	Enable this Content Disarm and Reconstruction feature.		
pdf-embedfile	Enable/disable stripping of embedded files in PDF documents.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable this Content Disarm and Reconstruction feature.		
	<i>enable</i>	Enable this Content Disarm and Reconstruction feature.		
pdf-hyperlink	Enable/disable stripping of hyperlinks from PDF documents.	option	-	enable



Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable this Content Disarm and Reconstruction feature.		
	<i>enable</i>	Enable this Content Disarm and Reconstruction feature.		
pdf-act-gotor	Enable/disable stripping of PDF document actions that access other PDF documents.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable this Content Disarm and Reconstruction feature.		
	<i>enable</i>	Enable this Content Disarm and Reconstruction feature.		
pdf-act-launch	Enable/disable stripping of PDF document actions that launch other applications.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable this Content Disarm and Reconstruction feature.		
	<i>enable</i>	Enable this Content Disarm and Reconstruction feature.		
pdf-act-sound	Enable/disable stripping of PDF document actions that play a sound.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable this Content Disarm and Reconstruction feature.		
	<i>enable</i>	Enable this Content Disarm and Reconstruction feature.		
pdf-act-movie	Enable/disable stripping of PDF document actions that play a movie.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable this Content Disarm and Reconstruction feature.		
	<i>enable</i>	Enable this Content Disarm and Reconstruction feature.		
pdf-act-java	Enable/disable stripping of PDF document actions that execute JavaScript code.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable this Content Disarm and Reconstruction feature.		
	<i>enable</i>	Enable this Content Disarm and Reconstruction feature.		
pdf-act-form	Enable/disable stripping of PDF document actions that submit data to other targets.	option	-	enable

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable this Content Disarm and Reconstruction feature.		
	<i>enable</i>	Enable this Content Disarm and Reconstruction feature.		
cover-page	Enable/disable inserting a cover page into the disarmed document.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable this Content Disarm and Reconstruction feature.		
	<i>enable</i>	Enable this Content Disarm and Reconstruction feature.		
detect-only	Enable/disable only detect disarmable files, do not alter content.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable this Content Disarm and Reconstruction feature.		
	<i>enable</i>	Enable this Content Disarm and Reconstruction feature.		

## config ftp

Parameter	Description	Type	Size	Default
av-scan	Enable AntiVirus scan service.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable.		
	<i>block</i>	Block the virus infected files.		
	<i>monitor</i>	Log the virus infected files.		
outbreak-prevention	Enable virus outbreak prevention service.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable.		
	<i>block</i>	Block the matched files.		
	<i>monitor</i>	Log the matched files.		
external-blocklist	Enable external-blocklist. Analyzes files including the content of archives.	option	-	disable

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable.		
	<i>block</i>	Block the matched files.		
	<i>monitor</i>	Log the matched files.		
fortindr	Enable/disable scanning of files by FortiNDR.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable.		
	<i>block</i>	Block the FortiNDR detected infections.		
	<i>monitor</i>	Log the FortiNDR detected infections.		
quarantine	Enable/disable quarantine for infected files.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable quarantine for infected files.		
	<i>enable</i>	Enable quarantine for infected files.		
archive-block	Select the archive types to block.	option	-	
	<b>Option</b>	<b>Description</b>		
	<i>encrypted</i>	Block encrypted archives.		
	<i>corrupted</i>	Block corrupted archives.		
	<i>partiallycorrupted</i>	Block partially corrupted archives.		
	<i>multipart</i>	Block multipart archives.		
	<i>nested</i>	Block nested archives that exceed uncompressed nest limit.		
	<i>mailbomb</i>	Block mail bomb archives.		
	<i>timeout</i>	Block scan timeout.		
	<i>unhandled</i>	Block archives that FortiOS cannot open.		
archive-log	Select the archive types to log.	option	-	
	<b>Option</b>	<b>Description</b>		
	<i>encrypted</i>	Log encrypted archives.		
	<i>corrupted</i>	Log corrupted archives.		
	<i>partiallycorrupted</i>	Log partially corrupted archives.		

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>multipart</i>	Log multipart archives.		
	<i>nested</i>	Log nested archives that exceed uncompressed nest limit.		
	<i>mailbomb</i>	Log mail bomb archives.		
	<i>timeout</i>	Log scan timeout.		
	<i>unhandled</i>	Log archives that FortiOS cannot open.		
emulator	Enable/disable the virus emulator.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable the virus emulator.		
	<i>disable</i>	Disable the virus emulator.		

## config http

Parameter	Description	Type	Size	Default
av-scan	Enable AntiVirus scan service.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable.		
	<i>block</i>	Block the virus infected files.		
	<i>monitor</i>	Log the virus infected files.		
outbreak-prevention	Enable virus outbreak prevention service.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable.		
	<i>block</i>	Block the matched files.		
	<i>monitor</i>	Log the matched files.		
external-blocklist	Enable external-blocklist. Analyzes files including the content of archives.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable.		
	<i>block</i>	Block the matched files.		
	<i>monitor</i>	Log the matched files.		

Parameter	Description	Type	Size	Default
fortindr	Enable/disable scanning of files by FortiNDR.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable.		
	<i>block</i>	Block the FortiNDR detected infections.		
	<i>monitor</i>	Log the FortiNDR detected infections.		
quarantine	Enable/disable quarantine for infected files.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable quarantine for infected files.		
	<i>enable</i>	Enable quarantine for infected files.		
archive-block	Select the archive types to block.	option	-	
	<b>Option</b>	<b>Description</b>		
	<i>encrypted</i>	Block encrypted archives.		
	<i>corrupted</i>	Block corrupted archives.		
	<i>partiallycorrupted</i>	Block partially corrupted archives.		
	<i>multipart</i>	Block multipart archives.		
	<i>nested</i>	Block nested archives that exceed uncompressed nest limit.		
	<i>mailbomb</i>	Block mail bomb archives.		
	<i>timeout</i>	Block scan timeout.		
	<i>unhandled</i>	Block archives that FortiOS cannot open.		
archive-log	Select the archive types to log.	option	-	
	<b>Option</b>	<b>Description</b>		
	<i>encrypted</i>	Log encrypted archives.		
	<i>corrupted</i>	Log corrupted archives.		
	<i>partiallycorrupted</i>	Log partially corrupted archives.		
	<i>multipart</i>	Log multipart archives.		
	<i>nested</i>	Log nested archives that exceed uncompressed nest limit.		
	<i>mailbomb</i>	Log mail bomb archives.		
	<i>timeout</i>	Log scan timeout.		
<i>unhandled</i>	Log archives that FortiOS cannot open.			

Parameter	Description	Type	Size	Default
emulator	Enable/disable the virus emulator.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable the virus emulator.		
	<i>disable</i>	Disable the virus emulator.		
unknown-content-encoding	Configure the action the FortiGate unit will take on unknown content-encoding.	option	-	block
	<b>Option</b>	<b>Description</b>		
	<i>block</i>	Block HTTP session when unknown content-encoding is detected.		
	<i>inspect</i>	Inspect HTTP traffic as plain-text with AV scan when unknown content-encoding is detected.		
	<i>bypass</i>	Bypass AV scan when unknown content-encoding is detected.		
content-disarm	Enable/disable Content Disarm and Reconstruction when performing AntiVirus scan.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable Content Disarm and Reconstruction when performing AntiVirus scan.		
	<i>enable</i>	Enable Content Disarm and Reconstruction when performing AntiVirus scan.		

## config imap

Parameter	Description	Type	Size	Default
av-scan	Enable AntiVirus scan service.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable.		
	<i>block</i>	Block the virus infected files.		
	<i>monitor</i>	Log the virus infected files.		
outbreak-prevention	Enable virus outbreak prevention service.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable.		
	<i>block</i>	Block the matched files.		
	<i>monitor</i>	Log the matched files.		

Parameter	Description	Type	Size	Default																		
external-blocklist	Enable external-blocklist. Analyzes files including the content of archives.	option	-	disable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable.</td></tr><tr><td><i>block</i></td><td>Block the matched files.</td></tr><tr><td><i>monitor</i></td><td>Log the matched files.</td></tr></table>	Option	Description	<i>disable</i>	Disable.	<i>block</i>	Block the matched files.	<i>monitor</i>	Log the matched files.													
Option	Description																					
<i>disable</i>	Disable.																					
<i>block</i>	Block the matched files.																					
<i>monitor</i>	Log the matched files.																					
fortindr	Enable/disable scanning of files by FortiNDR.	option	-	disable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable.</td></tr><tr><td><i>block</i></td><td>Block the FortiNDR detected infections.</td></tr><tr><td><i>monitor</i></td><td>Log the FortiNDR detected infections.</td></tr></table>	Option	Description	<i>disable</i>	Disable.	<i>block</i>	Block the FortiNDR detected infections.	<i>monitor</i>	Log the FortiNDR detected infections.													
Option	Description																					
<i>disable</i>	Disable.																					
<i>block</i>	Block the FortiNDR detected infections.																					
<i>monitor</i>	Log the FortiNDR detected infections.																					
quarantine	Enable/disable quarantine for infected files.	option	-	disable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable quarantine for infected files.</td></tr><tr><td><i>enable</i></td><td>Enable quarantine for infected files.</td></tr></table>	Option	Description	<i>disable</i>	Disable quarantine for infected files.	<i>enable</i>	Enable quarantine for infected files.															
Option	Description																					
<i>disable</i>	Disable quarantine for infected files.																					
<i>enable</i>	Enable quarantine for infected files.																					
archive-block	Select the archive types to block.	option	-																			
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>encrypted</i></td><td>Block encrypted archives.</td></tr><tr><td><i>corrupted</i></td><td>Block corrupted archives.</td></tr><tr><td><i>partiallycorrupted</i></td><td>Block partially corrupted archives.</td></tr><tr><td><i>multipart</i></td><td>Block multipart archives.</td></tr><tr><td><i>nested</i></td><td>Block nested archives that exceed uncompressed nest limit.</td></tr><tr><td><i>mailbomb</i></td><td>Block mail bomb archives.</td></tr><tr><td><i>timeout</i></td><td>Block scan timeout.</td></tr><tr><td><i>unhandled</i></td><td>Block archives that FortiOS cannot open.</td></tr></table>	Option	Description	<i>encrypted</i>	Block encrypted archives.	<i>corrupted</i>	Block corrupted archives.	<i>partiallycorrupted</i>	Block partially corrupted archives.	<i>multipart</i>	Block multipart archives.	<i>nested</i>	Block nested archives that exceed uncompressed nest limit.	<i>mailbomb</i>	Block mail bomb archives.	<i>timeout</i>	Block scan timeout.	<i>unhandled</i>	Block archives that FortiOS cannot open.			
Option	Description																					
<i>encrypted</i>	Block encrypted archives.																					
<i>corrupted</i>	Block corrupted archives.																					
<i>partiallycorrupted</i>	Block partially corrupted archives.																					
<i>multipart</i>	Block multipart archives.																					
<i>nested</i>	Block nested archives that exceed uncompressed nest limit.																					
<i>mailbomb</i>	Block mail bomb archives.																					
<i>timeout</i>	Block scan timeout.																					
<i>unhandled</i>	Block archives that FortiOS cannot open.																					
archive-log	Select the archive types to log.	option	-																			
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>encrypted</i></td><td>Log encrypted archives.</td></tr></table>	Option	Description	<i>encrypted</i>	Log encrypted archives.																	
Option	Description																					
<i>encrypted</i>	Log encrypted archives.																					

Parameter	Description	Type	Size	Default																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>corrupted</i></td><td>Log corrupted archives.</td></tr><tr><td><i>partiallycorrupted</i></td><td>Log partially corrupted archives.</td></tr><tr><td><i>multipart</i></td><td>Log multipart archives.</td></tr><tr><td><i>nested</i></td><td>Log nested archives that exceed uncompressed nest limit.</td></tr><tr><td><i>mailbomb</i></td><td>Log mail bomb archives.</td></tr><tr><td><i>timeout</i></td><td>Log scan timeout.</td></tr><tr><td><i>unhandled</i></td><td>Log archives that FortiOS cannot open.</td></tr></table>	Option	Description	<i>corrupted</i>	Log corrupted archives.	<i>partiallycorrupted</i>	Log partially corrupted archives.	<i>multipart</i>	Log multipart archives.	<i>nested</i>	Log nested archives that exceed uncompressed nest limit.	<i>mailbomb</i>	Log mail bomb archives.	<i>timeout</i>	Log scan timeout.	<i>unhandled</i>	Log archives that FortiOS cannot open.			
	Option	Description																		
	<i>corrupted</i>	Log corrupted archives.																		
	<i>partiallycorrupted</i>	Log partially corrupted archives.																		
	<i>multipart</i>	Log multipart archives.																		
	<i>nested</i>	Log nested archives that exceed uncompressed nest limit.																		
	<i>mailbomb</i>	Log mail bomb archives.																		
	<i>timeout</i>	Log scan timeout.																		
<i>unhandled</i>	Log archives that FortiOS cannot open.																			
emulator	Enable/disable the virus emulator.	option	-	enable																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable the virus emulator.</td></tr><tr><td><i>disable</i></td><td>Disable the virus emulator.</td></tr></table>	Option	Description	<i>enable</i>	Enable the virus emulator.	<i>disable</i>	Disable the virus emulator.													
	Option	Description																		
	<i>enable</i>	Enable the virus emulator.																		
<i>disable</i>	Disable the virus emulator.																			
executables	Treat Windows executable files as viruses for the purpose of blocking or monitoring.	option	-	default																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>Perform standard AntiVirus scanning of Windows executable files.</td></tr><tr><td><i>virus</i></td><td>Treat Windows executables as viruses.</td></tr></table>	Option	Description	<i>default</i>	Perform standard AntiVirus scanning of Windows executable files.	<i>virus</i>	Treat Windows executables as viruses.													
	Option	Description																		
	<i>default</i>	Perform standard AntiVirus scanning of Windows executable files.																		
<i>virus</i>	Treat Windows executables as viruses.																			
content-disarm	Enable/disable Content Disarm and Reconstruction when performing AntiVirus scan.	option	-	disable																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable Content Disarm and Reconstruction when performing AntiVirus scan.</td></tr><tr><td><i>enable</i></td><td>Enable Content Disarm and Reconstruction when performing AntiVirus scan.</td></tr></table>	Option	Description	<i>disable</i>	Disable Content Disarm and Reconstruction when performing AntiVirus scan.	<i>enable</i>	Enable Content Disarm and Reconstruction when performing AntiVirus scan.													
	Option	Description																		
	<i>disable</i>	Disable Content Disarm and Reconstruction when performing AntiVirus scan.																		
<i>enable</i>	Enable Content Disarm and Reconstruction when performing AntiVirus scan.																			

## config mapi

Parameter	Description	Type	Size	Default
av-scan	Enable AntiVirus scan service.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable.		
	<i>block</i>	Block the virus infected files.		
	<i>monitor</i>	Log the virus infected files.		



Parameter	Description	Type	Size	Default																		
outbreak-prevention	Enable virus outbreak prevention service.	option	-	disable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable.</td></tr><tr><td><i>block</i></td><td>Block the matched files.</td></tr><tr><td><i>monitor</i></td><td>Log the matched files.</td></tr></table>	Option	Description	<i>disable</i>	Disable.	<i>block</i>	Block the matched files.	<i>monitor</i>	Log the matched files.													
Option	Description																					
<i>disable</i>	Disable.																					
<i>block</i>	Block the matched files.																					
<i>monitor</i>	Log the matched files.																					
external-blocklist	Enable external-blocklist. Analyzes files including the content of archives.	option	-	disable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable.</td></tr><tr><td><i>block</i></td><td>Block the matched files.</td></tr><tr><td><i>monitor</i></td><td>Log the matched files.</td></tr></table>	Option	Description	<i>disable</i>	Disable.	<i>block</i>	Block the matched files.	<i>monitor</i>	Log the matched files.													
Option	Description																					
<i>disable</i>	Disable.																					
<i>block</i>	Block the matched files.																					
<i>monitor</i>	Log the matched files.																					
quarantine	Enable/disable quarantine for infected files.	option	-	disable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable quarantine for infected files.</td></tr><tr><td><i>enable</i></td><td>Enable quarantine for infected files.</td></tr></table>	Option	Description	<i>disable</i>	Disable quarantine for infected files.	<i>enable</i>	Enable quarantine for infected files.															
Option	Description																					
<i>disable</i>	Disable quarantine for infected files.																					
<i>enable</i>	Enable quarantine for infected files.																					
archive-block	Select the archive types to block.	option	-																			
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>encrypted</i></td><td>Block encrypted archives.</td></tr><tr><td><i>corrupted</i></td><td>Block corrupted archives.</td></tr><tr><td><i>partiallycorrupted</i></td><td>Block partially corrupted archives.</td></tr><tr><td><i>multipart</i></td><td>Block multipart archives.</td></tr><tr><td><i>nested</i></td><td>Block nested archives that exceed uncompressed nest limit.</td></tr><tr><td><i>mailbomb</i></td><td>Block mail bomb archives.</td></tr><tr><td><i>timeout</i></td><td>Block scan timeout.</td></tr><tr><td><i>unhandled</i></td><td>Block archives that FortiOS cannot open.</td></tr></table>	Option	Description	<i>encrypted</i>	Block encrypted archives.	<i>corrupted</i>	Block corrupted archives.	<i>partiallycorrupted</i>	Block partially corrupted archives.	<i>multipart</i>	Block multipart archives.	<i>nested</i>	Block nested archives that exceed uncompressed nest limit.	<i>mailbomb</i>	Block mail bomb archives.	<i>timeout</i>	Block scan timeout.	<i>unhandled</i>	Block archives that FortiOS cannot open.			
Option	Description																					
<i>encrypted</i>	Block encrypted archives.																					
<i>corrupted</i>	Block corrupted archives.																					
<i>partiallycorrupted</i>	Block partially corrupted archives.																					
<i>multipart</i>	Block multipart archives.																					
<i>nested</i>	Block nested archives that exceed uncompressed nest limit.																					
<i>mailbomb</i>	Block mail bomb archives.																					
<i>timeout</i>	Block scan timeout.																					
<i>unhandled</i>	Block archives that FortiOS cannot open.																					
archive-log	Select the archive types to log.	option	-																			

Parameter	Description	Type	Size	Default																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>encrypted</i></td><td>Log encrypted archives.</td></tr><tr><td><i>corrupted</i></td><td>Log corrupted archives.</td></tr><tr><td><i>partiallycorrupted</i></td><td>Log partially corrupted archives.</td></tr><tr><td><i>multipart</i></td><td>Log multipart archives.</td></tr><tr><td><i>nested</i></td><td>Log nested archives that exceed uncompressed nest limit.</td></tr><tr><td><i>mailbomb</i></td><td>Log mail bomb archives.</td></tr><tr><td><i>timeout</i></td><td>Log scan timeout.</td></tr><tr><td><i>unhandled</i></td><td>Log archives that FortiOS cannot open.</td></tr></table>	Option	Description	<i>encrypted</i>	Log encrypted archives.	<i>corrupted</i>	Log corrupted archives.	<i>partiallycorrupted</i>	Log partially corrupted archives.	<i>multipart</i>	Log multipart archives.	<i>nested</i>	Log nested archives that exceed uncompressed nest limit.	<i>mailbomb</i>	Log mail bomb archives.	<i>timeout</i>	Log scan timeout.	<i>unhandled</i>	Log archives that FortiOS cannot open.			
	Option	Description																				
	<i>encrypted</i>	Log encrypted archives.																				
	<i>corrupted</i>	Log corrupted archives.																				
	<i>partiallycorrupted</i>	Log partially corrupted archives.																				
	<i>multipart</i>	Log multipart archives.																				
	<i>nested</i>	Log nested archives that exceed uncompressed nest limit.																				
	<i>mailbomb</i>	Log mail bomb archives.																				
	<i>timeout</i>	Log scan timeout.																				
<i>unhandled</i>	Log archives that FortiOS cannot open.																					
emulator	Enable/disable the virus emulator.	option	-	enable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable the virus emulator.</td></tr><tr><td><i>disable</i></td><td>Disable the virus emulator.</td></tr></table>	Option	Description	<i>enable</i>	Enable the virus emulator.	<i>disable</i>	Disable the virus emulator.															
	Option	Description																				
	<i>enable</i>	Enable the virus emulator.																				
<i>disable</i>	Disable the virus emulator.																					
executables	Treat Windows executable files as viruses for the purpose of blocking or monitoring.	option	-	default																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>Perform standard AntiVirus scanning of Windows executable files.</td></tr><tr><td><i>virus</i></td><td>Treat Windows executables as viruses.</td></tr></table>	Option	Description	<i>default</i>	Perform standard AntiVirus scanning of Windows executable files.	<i>virus</i>	Treat Windows executables as viruses.															
	Option	Description																				
	<i>default</i>	Perform standard AntiVirus scanning of Windows executable files.																				
<i>virus</i>	Treat Windows executables as viruses.																					

### config nac-quar

Parameter	Description	Type	Size	Default						
infected	Enable/Disable quarantining infected hosts to the banned user list.	option	-	none						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>Do not quarantine infected hosts.</td></tr><tr><td><i>quar-src-ip</i></td><td>Quarantine all traffic from the infected hosts source IP.</td></tr></table>				Option	Description	<i>none</i>	Do not quarantine infected hosts.	<i>quar-src-ip</i>	Quarantine all traffic from the infected hosts source IP.
Option	Description									
<i>none</i>	Do not quarantine infected hosts.									
<i>quar-src-ip</i>	Quarantine all traffic from the infected hosts source IP.									
expiry	Duration of quarantine.	user	Not Specified	5m						
log	Enable/disable AntiVirus quarantine logging.	option	-	disable						

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable AntiVirus quarantine logging.		
	<i>disable</i>	Disable AntiVirus quarantine logging.		

## config nntp

Parameter	Description	Type	Size	Default
av-scan	Enable AntiVirus scan service.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable.		
	<i>block</i>	Block the virus infected files.		
	<i>monitor</i>	Log the virus infected files.		
outbreak-prevention	Enable virus outbreak prevention service.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable.		
	<i>block</i>	Block the matched files.		
	<i>monitor</i>	Log the matched files.		
external-blocklist	Enable external-blocklist. Analyzes files including the content of archives.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable.		
	<i>block</i>	Block the matched files.		
	<i>monitor</i>	Log the matched files.		
fortindr	Enable/disable scanning of files by FortiNDR.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable.		
	<i>block</i>	Block the FortiNDR detected infections.		
	<i>monitor</i>	Log the FortiNDR detected infections.		
quarantine	Enable/disable quarantine for infected files.	option	-	disable

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable quarantine for infected files.		
	<i>enable</i>	Enable quarantine for infected files.		
archive-block	Select the archive types to block.	option	-	
	<b>Option</b>	<b>Description</b>		
	<i>encrypted</i>	Block encrypted archives.		
	<i>corrupted</i>	Block corrupted archives.		
	<i>partiallycorrupted</i>	Block partially corrupted archives.		
	<i>multipart</i>	Block multipart archives.		
	<i>nested</i>	Block nested archives that exceed uncompressed nest limit.		
	<i>mailbomb</i>	Block mail bomb archives.		
	<i>timeout</i>	Block scan timeout.		
	<i>unhandled</i>	Block archives that FortiOS cannot open.		
archive-log	Select the archive types to log.	option	-	
	<b>Option</b>	<b>Description</b>		
	<i>encrypted</i>	Log encrypted archives.		
	<i>corrupted</i>	Log corrupted archives.		
	<i>partiallycorrupted</i>	Log partially corrupted archives.		
	<i>multipart</i>	Log multipart archives.		
	<i>nested</i>	Log nested archives that exceed uncompressed nest limit.		
	<i>mailbomb</i>	Log mail bomb archives.		
	<i>timeout</i>	Log scan timeout.		
	<i>unhandled</i>	Log archives that FortiOS cannot open.		
emulator	Enable/disable the virus emulator.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable the virus emulator.		
	<i>disable</i>	Disable the virus emulator.		

## config pop3

Parameter	Description	Type	Size	Default
av-scan	Enable AntiVirus scan service.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable.		
	<i>block</i>	Block the virus infected files.		
	<i>monitor</i>	Log the virus infected files.		
outbreak-prevention	Enable virus outbreak prevention service.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable.		
	<i>block</i>	Block the matched files.		
	<i>monitor</i>	Log the matched files.		
external-blocklist	Enable external-blocklist. Analyzes files including the content of archives.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable.		
	<i>block</i>	Block the matched files.		
	<i>monitor</i>	Log the matched files.		
fortindr	Enable/disable scanning of files by FortiNDR.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable.		
	<i>block</i>	Block the FortiNDR detected infections.		
	<i>monitor</i>	Log the FortiNDR detected infections.		
quarantine	Enable/disable quarantine for infected files.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable quarantine for infected files.		
	<i>enable</i>	Enable quarantine for infected files.		
archive-block	Select the archive types to block.	option	-	

Parameter	Description	Type	Size	Default																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>encrypted</i></td><td>Block encrypted archives.</td></tr><tr><td><i>corrupted</i></td><td>Block corrupted archives.</td></tr><tr><td><i>partiallycorrupted</i></td><td>Block partially corrupted archives.</td></tr><tr><td><i>multipart</i></td><td>Block multipart archives.</td></tr><tr><td><i>nested</i></td><td>Block nested archives that exceed uncompressed nest limit.</td></tr><tr><td><i>mailbomb</i></td><td>Block mail bomb archives.</td></tr><tr><td><i>timeout</i></td><td>Block scan timeout.</td></tr><tr><td><i>unhandled</i></td><td>Block archives that FortiOS cannot open.</td></tr></table>	Option	Description	<i>encrypted</i>	Block encrypted archives.	<i>corrupted</i>	Block corrupted archives.	<i>partiallycorrupted</i>	Block partially corrupted archives.	<i>multipart</i>	Block multipart archives.	<i>nested</i>	Block nested archives that exceed uncompressed nest limit.	<i>mailbomb</i>	Block mail bomb archives.	<i>timeout</i>	Block scan timeout.	<i>unhandled</i>	Block archives that FortiOS cannot open.			
	Option	Description																				
	<i>encrypted</i>	Block encrypted archives.																				
	<i>corrupted</i>	Block corrupted archives.																				
	<i>partiallycorrupted</i>	Block partially corrupted archives.																				
	<i>multipart</i>	Block multipart archives.																				
	<i>nested</i>	Block nested archives that exceed uncompressed nest limit.																				
	<i>mailbomb</i>	Block mail bomb archives.																				
	<i>timeout</i>	Block scan timeout.																				
<i>unhandled</i>	Block archives that FortiOS cannot open.																					
archive-log	Select the archive types to log.	option	-																			
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>encrypted</i></td><td>Log encrypted archives.</td></tr><tr><td><i>corrupted</i></td><td>Log corrupted archives.</td></tr><tr><td><i>partiallycorrupted</i></td><td>Log partially corrupted archives.</td></tr><tr><td><i>multipart</i></td><td>Log multipart archives.</td></tr><tr><td><i>nested</i></td><td>Log nested archives that exceed uncompressed nest limit.</td></tr><tr><td><i>mailbomb</i></td><td>Log mail bomb archives.</td></tr><tr><td><i>timeout</i></td><td>Log scan timeout.</td></tr><tr><td><i>unhandled</i></td><td>Log archives that FortiOS cannot open.</td></tr></table>	Option	Description	<i>encrypted</i>	Log encrypted archives.	<i>corrupted</i>	Log corrupted archives.	<i>partiallycorrupted</i>	Log partially corrupted archives.	<i>multipart</i>	Log multipart archives.	<i>nested</i>	Log nested archives that exceed uncompressed nest limit.	<i>mailbomb</i>	Log mail bomb archives.	<i>timeout</i>	Log scan timeout.	<i>unhandled</i>	Log archives that FortiOS cannot open.			
	Option	Description																				
	<i>encrypted</i>	Log encrypted archives.																				
	<i>corrupted</i>	Log corrupted archives.																				
	<i>partiallycorrupted</i>	Log partially corrupted archives.																				
	<i>multipart</i>	Log multipart archives.																				
	<i>nested</i>	Log nested archives that exceed uncompressed nest limit.																				
	<i>mailbomb</i>	Log mail bomb archives.																				
	<i>timeout</i>	Log scan timeout.																				
<i>unhandled</i>	Log archives that FortiOS cannot open.																					
emulator	Enable/disable the virus emulator.	option	-	enable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable the virus emulator.</td></tr><tr><td><i>disable</i></td><td>Disable the virus emulator.</td></tr></table>	Option	Description	<i>enable</i>	Enable the virus emulator.	<i>disable</i>	Disable the virus emulator.															
	Option	Description																				
	<i>enable</i>	Enable the virus emulator.																				
<i>disable</i>	Disable the virus emulator.																					
executables	Treat Windows executable files as viruses for the purpose of blocking or monitoring.	option	-	default																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>Perform standard AntiVirus scanning of Windows executable files.</td></tr><tr><td><i>virus</i></td><td>Treat Windows executables as viruses.</td></tr></table>	Option	Description	<i>default</i>	Perform standard AntiVirus scanning of Windows executable files.	<i>virus</i>	Treat Windows executables as viruses.															
	Option	Description																				
	<i>default</i>	Perform standard AntiVirus scanning of Windows executable files.																				
<i>virus</i>	Treat Windows executables as viruses.																					

Parameter	Description	Type	Size	Default						
content-disarm	Enable/disable Content Disarm and Reconstruction when performing AntiVirus scan.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable Content Disarm and Reconstruction when performing AntiVirus scan.</td></tr><tr><td><i>enable</i></td><td>Enable Content Disarm and Reconstruction when performing AntiVirus scan.</td></tr></table>	Option	Description	<i>disable</i>	Disable Content Disarm and Reconstruction when performing AntiVirus scan.	<i>enable</i>	Enable Content Disarm and Reconstruction when performing AntiVirus scan.			
Option	Description									
<i>disable</i>	Disable Content Disarm and Reconstruction when performing AntiVirus scan.									
<i>enable</i>	Enable Content Disarm and Reconstruction when performing AntiVirus scan.									

## config smtp

Parameter	Description	Type	Size	Default								
av-scan	Enable AntiVirus scan service.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable.</td></tr><tr><td><i>block</i></td><td>Block the virus infected files.</td></tr><tr><td><i>monitor</i></td><td>Log the virus infected files.</td></tr></table>	Option	Description	<i>disable</i>	Disable.	<i>block</i>	Block the virus infected files.	<i>monitor</i>	Log the virus infected files.			
Option	Description											
<i>disable</i>	Disable.											
<i>block</i>	Block the virus infected files.											
<i>monitor</i>	Log the virus infected files.											
outbreak-prevention	Enable virus outbreak prevention service.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable.</td></tr><tr><td><i>block</i></td><td>Block the matched files.</td></tr><tr><td><i>monitor</i></td><td>Log the matched files.</td></tr></table>	Option	Description	<i>disable</i>	Disable.	<i>block</i>	Block the matched files.	<i>monitor</i>	Log the matched files.			
Option	Description											
<i>disable</i>	Disable.											
<i>block</i>	Block the matched files.											
<i>monitor</i>	Log the matched files.											
external-blocklist	Enable external-blocklist. Analyzes files including the content of archives.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable.</td></tr><tr><td><i>block</i></td><td>Block the matched files.</td></tr><tr><td><i>monitor</i></td><td>Log the matched files.</td></tr></table>	Option	Description	<i>disable</i>	Disable.	<i>block</i>	Block the matched files.	<i>monitor</i>	Log the matched files.			
Option	Description											
<i>disable</i>	Disable.											
<i>block</i>	Block the matched files.											
<i>monitor</i>	Log the matched files.											
fortindr	Enable/disable scanning of files by FortiNDR.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable.</td></tr><tr><td><i>block</i></td><td>Block the FortiNDR detected infections.</td></tr><tr><td><i>monitor</i></td><td>Log the FortiNDR detected infections.</td></tr></table>	Option	Description	<i>disable</i>	Disable.	<i>block</i>	Block the FortiNDR detected infections.	<i>monitor</i>	Log the FortiNDR detected infections.			
Option	Description											
<i>disable</i>	Disable.											
<i>block</i>	Block the FortiNDR detected infections.											
<i>monitor</i>	Log the FortiNDR detected infections.											

Parameter	Description	Type	Size	Default
quarantine	Enable/disable quarantine for infected files.	option	-	disable
	<b>Option</b> <b>Description</b>			
	<i>disable</i>	Disable quarantine for infected files.		
	<i>enable</i>	Enable quarantine for infected files.		
archive-block	Select the archive types to block.	option	-	
	<b>Option</b> <b>Description</b>			
	<i>encrypted</i>	Block encrypted archives.		
	<i>corrupted</i>	Block corrupted archives.		
	<i>partiallycorrupted</i>	Block partially corrupted archives.		
	<i>multipart</i>	Block multipart archives.		
	<i>nested</i>	Block nested archives that exceed uncompressed nest limit.		
	<i>mailbomb</i>	Block mail bomb archives.		
	<i>timeout</i>	Block scan timeout.		
	<i>unhandled</i>	Block archives that FortiOS cannot open.		
archive-log	Select the archive types to log.	option	-	
	<b>Option</b> <b>Description</b>			
	<i>encrypted</i>	Log encrypted archives.		
	<i>corrupted</i>	Log corrupted archives.		
	<i>partiallycorrupted</i>	Log partially corrupted archives.		
	<i>multipart</i>	Log multipart archives.		
	<i>nested</i>	Log nested archives that exceed uncompressed nest limit.		
	<i>mailbomb</i>	Log mail bomb archives.		
	<i>timeout</i>	Log scan timeout.		
	<i>unhandled</i>	Log archives that FortiOS cannot open.		
emulator	Enable/disable the virus emulator.	option	-	enable
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Enable the virus emulator.		
	<i>disable</i>	Disable the virus emulator.		



Parameter	Description	Type	Size	Default						
executables	Treat Windows executable files as viruses for the purpose of blocking or monitoring.	option	-	default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>Perform standard AntiVirus scanning of Windows executable files.</td></tr><tr><td><i>virus</i></td><td>Treat Windows executables as viruses.</td></tr></table>	Option	Description	<i>default</i>	Perform standard AntiVirus scanning of Windows executable files.	<i>virus</i>	Treat Windows executables as viruses.			
Option	Description									
<i>default</i>	Perform standard AntiVirus scanning of Windows executable files.									
<i>virus</i>	Treat Windows executables as viruses.									
content-disarm	Enable/disable Content Disarm and Reconstruction when performing AntiVirus scan.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable Content Disarm and Reconstruction when performing AntiVirus scan.</td></tr><tr><td><i>enable</i></td><td>Enable Content Disarm and Reconstruction when performing AntiVirus scan.</td></tr></table>	Option	Description	<i>disable</i>	Disable Content Disarm and Reconstruction when performing AntiVirus scan.	<i>enable</i>	Enable Content Disarm and Reconstruction when performing AntiVirus scan.			
Option	Description									
<i>disable</i>	Disable Content Disarm and Reconstruction when performing AntiVirus scan.									
<i>enable</i>	Enable Content Disarm and Reconstruction when performing AntiVirus scan.									

## config ssh

Parameter	Description	Type	Size	Default
av-scan	Enable AntiVirus scan service.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable.		
	<i>block</i>	Block the virus infected files.		
	<i>monitor</i>	Log the virus infected files.		
outbreak-prevention	Enable virus outbreak prevention service.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable.		
	<i>block</i>	Block the matched files.		
	<i>monitor</i>	Log the matched files.		
external-blocklist	Enable external-blocklist. Analyzes files including the content of archives.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable.		
	<i>block</i>	Block the matched files.		
	<i>monitor</i>	Log the matched files.		

Parameter	Description	Type	Size	Default
fortindr	Enable/disable scanning of files by FortiNDR.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable.		
	<i>block</i>	Block the FortiNDR detected infections.		
	<i>monitor</i>	Log the FortiNDR detected infections.		
quarantine	Enable/disable quarantine for infected files.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable quarantine for infected files.		
	<i>enable</i>	Enable quarantine for infected files.		
archive-block	Select the archive types to block.	option	-	
	<b>Option</b>	<b>Description</b>		
	<i>encrypted</i>	Block encrypted archives.		
	<i>corrupted</i>	Block corrupted archives.		
	<i>partiallycorrupted</i>	Block partially corrupted archives.		
	<i>multipart</i>	Block multipart archives.		
	<i>nested</i>	Block nested archives that exceed uncompressed nest limit.		
	<i>mailbomb</i>	Block mail bomb archives.		
	<i>timeout</i>	Block scan timeout.		
	<i>unhandled</i>	Block archives that FortiOS cannot open.		
archive-log	Select the archive types to log.	option	-	
	<b>Option</b>	<b>Description</b>		
	<i>encrypted</i>	Log encrypted archives.		
	<i>corrupted</i>	Log corrupted archives.		
	<i>partiallycorrupted</i>	Log partially corrupted archives.		
	<i>multipart</i>	Log multipart archives.		
	<i>nested</i>	Log nested archives that exceed uncompressed nest limit.		
	<i>mailbomb</i>	Log mail bomb archives.		
	<i>timeout</i>	Log scan timeout.		
<i>unhandled</i>	Log archives that FortiOS cannot open.			

Parameter	Description	Type	Size	Default
emulator	Enable/disable the virus emulator.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable the virus emulator.		
	<i>disable</i>	Disable the virus emulator.		

## config antivirus quarantine

Configure quarantine options.

```
config antivirus quarantine
  Description: Configure quarantine options.
  set agelimit {integer}
  set destination [NULL|disk|...]
  set drop-blocked {option1}, {option2}, ...
  set drop-infected {option1}, {option2}, ...
  set drop-machine-learning {option1}, {option2}, ...
  set lowspace [drop-new|ovrw-old]
  set maxfilesize {integer}
  set quarantine-quota {integer}
  set store-blocked {option1}, {option2}, ...
  set store-infected {option1}, {option2}, ...
  set store-machine-learning {option1}, {option2}, ...
end
```

## config antivirus quarantine

Parameter	Description	Type	Size	Default
agelimit	Age limit for quarantined files.	integer	Minimum value: 0 Maximum value: 479	0
destination	Choose whether to quarantine files to the FortiGate disk or to FortiAnalyzer or to delete them instead of quarantining them.	option	-	disk **
	<b>Option</b>	<b>Description</b>		
	<i>NULL</i>	Files that would be quarantined are deleted.		
	<i>disk</i>	Quarantine files to the FortiGate hard disk.		
	<i>FortiAnalyzer</i>	FortiAnalyzer		

Parameter	Description	Type	Size	Default																												
drop-blocked	Do not quarantine dropped files found in sessions using the selected protocols. Dropped files are deleted instead of being quarantined.	option	-																													
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>imap</td><td>IMAP.</td></tr><tr><td>smtp</td><td>SMTP.</td></tr><tr><td>pop3</td><td>POP3.</td></tr><tr><td>http</td><td>HTTP.</td></tr><tr><td>ftp</td><td>FTP.</td></tr><tr><td>nntp</td><td>NNTP.</td></tr><tr><td>imaps</td><td>IMAPS.</td></tr><tr><td>smtps</td><td>SMTPS.</td></tr><tr><td>pop3s</td><td>POP3S.</td></tr><tr><td>ftps</td><td>FTPS.</td></tr><tr><td>mapi</td><td>MAPI.</td></tr><tr><td>cifs</td><td>CIFS.</td></tr><tr><td>ssh</td><td>SSH.</td></tr></table>	Option	Description	imap	IMAP.	smtp	SMTP.	pop3	POP3.	http	HTTP.	ftp	FTP.	nntp	NNTP.	imaps	IMAPS.	smtps	SMTPS.	pop3s	POP3S.	ftps	FTPS.	mapi	MAPI.	cifs	CIFS.	ssh	SSH.			
	Option	Description																														
	imap	IMAP.																														
	smtp	SMTP.																														
	pop3	POP3.																														
	http	HTTP.																														
	ftp	FTP.																														
	nntp	NNTP.																														
	imaps	IMAPS.																														
	smtps	SMTPS.																														
	pop3s	POP3S.																														
	ftps	FTPS.																														
	mapi	MAPI.																														
	cifs	CIFS.																														
ssh	SSH.																															
drop-infected	Do not quarantine infected files found in sessions using the selected protocols. Dropped files are deleted instead of being quarantined.	option	-																													
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>imap</td><td>IMAP.</td></tr><tr><td>smtp</td><td>SMTP.</td></tr><tr><td>pop3</td><td>POP3.</td></tr><tr><td>http</td><td>HTTP.</td></tr><tr><td>ftp</td><td>FTP.</td></tr><tr><td>nntp</td><td>NNTP.</td></tr><tr><td>imaps</td><td>IMAPS.</td></tr><tr><td>smtps</td><td>SMTPS.</td></tr><tr><td>pop3s</td><td>POP3S.</td></tr></table>	Option	Description	imap	IMAP.	smtp	SMTP.	pop3	POP3.	http	HTTP.	ftp	FTP.	nntp	NNTP.	imaps	IMAPS.	smtps	SMTPS.	pop3s	POP3S.											
	Option	Description																														
	imap	IMAP.																														
	smtp	SMTP.																														
	pop3	POP3.																														
	http	HTTP.																														
	ftp	FTP.																														
	nntp	NNTP.																														
	imaps	IMAPS.																														
	smtps	SMTPS.																														
pop3s	POP3S.																															

Parameter	Description	Type	Size	Default																														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>https</i></td><td>HTTPS.</td></tr><tr><td><i>ftps</i></td><td>FTPS.</td></tr><tr><td><i>mapi</i></td><td>MAPI.</td></tr><tr><td><i>cifs</i></td><td>CIFS.</td></tr><tr><td><i>ssh</i></td><td>SSH.</td></tr></table>	Option	Description	<i>https</i>	HTTPS.	<i>ftps</i>	FTPS.	<i>mapi</i>	MAPI.	<i>cifs</i>	CIFS.	<i>ssh</i>	SSH.																					
	Option	Description																																
	<i>https</i>	HTTPS.																																
	<i>ftps</i>	FTPS.																																
	<i>mapi</i>	MAPI.																																
	<i>cifs</i>	CIFS.																																
	<i>ssh</i>	SSH.																																
drop-machine-learning	Do not quarantine files detected by machine learning found in sessions using the selected protocols. Dropped files are deleted instead of being quarantined.	option	-																															
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>imap</i></td><td>IMAP.</td></tr><tr><td><i>smtp</i></td><td>SMTP.</td></tr><tr><td><i>pop3</i></td><td>POP3.</td></tr><tr><td><i>http</i></td><td>HTTP.</td></tr><tr><td><i>ftp</i></td><td>FTP.</td></tr><tr><td><i>nnntp</i></td><td>NNTP.</td></tr><tr><td><i>imaps</i></td><td>IMAPS.</td></tr><tr><td><i>smtps</i></td><td>SMTPS.</td></tr><tr><td><i>pop3s</i></td><td>POP3S.</td></tr><tr><td><i>https</i></td><td>HTTPS.</td></tr><tr><td><i>ftps</i></td><td>FTPS.</td></tr><tr><td><i>mapi</i></td><td>MAPI.</td></tr><tr><td><i>cifs</i></td><td>CIFS.</td></tr><tr><td><i>ssh</i></td><td>SSH.</td></tr></table>	Option	Description	<i>imap</i>	IMAP.	<i>smtp</i>	SMTP.	<i>pop3</i>	POP3.	<i>http</i>	HTTP.	<i>ftp</i>	FTP.	<i>nnntp</i>	NNTP.	<i>imaps</i>	IMAPS.	<i>smtps</i>	SMTPS.	<i>pop3s</i>	POP3S.	<i>https</i>	HTTPS.	<i>ftps</i>	FTPS.	<i>mapi</i>	MAPI.	<i>cifs</i>	CIFS.	<i>ssh</i>	SSH.			
	Option	Description																																
	<i>imap</i>	IMAP.																																
	<i>smtp</i>	SMTP.																																
	<i>pop3</i>	POP3.																																
	<i>http</i>	HTTP.																																
	<i>ftp</i>	FTP.																																
	<i>nnntp</i>	NNTP.																																
	<i>imaps</i>	IMAPS.																																
	<i>smtps</i>	SMTPS.																																
	<i>pop3s</i>	POP3S.																																
	<i>https</i>	HTTPS.																																
	<i>ftps</i>	FTPS.																																
	<i>mapi</i>	MAPI.																																
	<i>cifs</i>	CIFS.																																
<i>ssh</i>	SSH.																																	
lowspace	Select the method for handling additional files when running low on disk space.	option	-	ovrw-old																														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>drop-new</i></td><td>Drop (delete) the most recently quarantined files.</td></tr><tr><td><i>ovrw-old</i></td><td>Overwrite the oldest quarantined files. That is, the files that are closest to being deleted from the quarantine.</td></tr></table>	Option	Description	<i>drop-new</i>	Drop (delete) the most recently quarantined files.	<i>ovrw-old</i>	Overwrite the oldest quarantined files. That is, the files that are closest to being deleted from the quarantine.																											
	Option	Description																																
	<i>drop-new</i>	Drop (delete) the most recently quarantined files.																																
<i>ovrw-old</i>	Overwrite the oldest quarantined files. That is, the files that are closest to being deleted from the quarantine.																																	

Parameter	Description	Type	Size	Default
maxfilesize	Maximum file size to quarantine.	integer	Minimum value: 0 Maximum value: 500	0
quarantine-quota	The amount of disk space to reserve for quarantining files.	integer	Minimum value: 0 Maximum value: 4294967295	0
store-blocked	Quarantine blocked files found in sessions using the selected protocols.	option	-	imap smtp pop3 http ftp nntp imaps smtps pop3s ftps mapi cifs ssh
	Option	Description		
	imap	IMAP.		
	smtp	SMTP.		
	pop3	POP3.		
	http	HTTP.		
	ftp	FTP.		
	nntp	NNTP.		
	imaps	IMAPS.		
	smtps	SMTPS.		
	pop3s	POP3S.		
	ftps	FTPS.		
	mapi	MAPI.		
	cifs	CIFS.		
	ssh	SSH.		

Parameter	Description	Type	Size	Default
store-infected	Quarantine infected files found in sessions using the selected protocols.	option	-	imap smtp pop3 http ftp nntp imaps smtps pop3s https ftps mapi cifs ssh
	<div><div>Option</div><div>Description</div></div>			
	imap	IMAP.		
	smtp	SMTP.		
	pop3	POP3.		
	http	HTTP.		
	ftp	FTP.		
	nntp	NNTP.		
	imaps	IMAPS.		
	smtps	SMTPS.		
	pop3s	POP3S.		
	https	HTTPS.		
	ftps	FTPS.		
	mapi	MAPI.		
	cifs	CIFS.		
ssh	SSH.			
store-machine-learning	Quarantine files detected by machine learning found in sessions using the selected protocols.	option	-	imap smtp pop3 http ftp nntp imaps smtps pop3s https ftps mapi cifs ssh
	<div><div>Option</div><div>Description</div></div>			
	imap	IMAP.		

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>smtp</i>	SMTP.		
	<i>pop3</i>	POP3.		
	<i>http</i>	HTTP.		
	<i>ftp</i>	FTP.		
	<i>nnntp</i>	NNTP.		
	<i>imaps</i>	IMAPS.		
	<i>smtps</i>	SMTPS.		
	<i>pop3s</i>	POP3S.		
	<i>https</i>	HTTPS.		
	<i>ftps</i>	FTPS.		
	<i>mapi</i>	MAPI.		
	<i>cifs</i>	CIFS.		
	<i>ssh</i>	SSH.		

\*\* Values may differ between models.

## config antivirus settings

Configure AntiVirus settings.

```
config antivirus settings
    Description: Configure AntiVirus settings.
    set cache-infected-result [enable|disable]
    set grayware [enable|disable]
    set machine-learning-detection [enable|monitor|...]
    set override-timeout {integer}
    set use-extreme-db [enable|disable]
end
```

## config antivirus settings

Parameter	Description	Type	Size	Default
cache-infected-result	Enable/disable cache of infected scan results.	option	-	enable



Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable cache of infected scan results.		
	<i>disable</i>	Disable cache of infected scan results.		
grayware	Enable/disable grayware detection when an AntiVirus profile is applied to traffic.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable grayware detection.		
	<i>disable</i>	Disable grayware detection.		
machine-learning-detection	Use machine learning based malware detection.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable machine learning based malware detection.		
	<i>monitor</i>	Enable machine learning based malware detection for monitoring only.		
	<i>disable</i>	Disable machine learning based malware detection.		
override-timeout	Override the large file scan timeout value in seconds. Zero is the default value and is used to disable this command. When disabled, the daemon adjusts the large file scan timeout based on the file size.	integer	Minimum value: 30 Maximum value: 3600	0
use-extreme-db	Enable/disable the use of Extreme AVDB.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable extreme AVDB.		
	<i>disable</i>	Disable extreme AVDB.		

## application

This section includes syntax for the following commands:

- [config application custom on page 62](#)
- [config application group on page 63](#)
- [config application list on page 64](#)
- [config application name on page 73](#)
- [config application rule-settings on page 75](#)

### config application custom

Configure custom application signatures.

```
config application custom
  Description: Configure custom application signatures.
  edit <tag>
    set behavior {user}
    set category {integer}
    set comment {string}
    set id {integer}
    set protocol {user}
    set signature {var-string}
    set technology {user}
    set vendor {user}
  next
end
```

### config application custom

Parameter	Description	Type	Size	Default
behavior	Custom application signature behavior.	user	Not Specified	
category	Custom application category ID (use ? to view available options).	integer	Minimum value: 0 Maximum value: 4294967295	0
comment	Comment.	string	Maximum length: 63	

Parameter	Description	Type	Size	Default
id	Custom application category ID (use ? to view available options).	integer	Minimum value: 0 Maximum value: 4294967295	0
protocol	Custom application signature protocol.	user	Not Specified	
signature	The text that makes up the actual custom application signature.	var-string	Maximum length: 4095	
tag	Signature tag.	string	Maximum length: 63	
technology	Custom application signature technology.	user	Not Specified	
vendor	Custom application signature vendor.	user	Not Specified	

## config application group

Configure firewall application groups.

```

config application group
    Description: Configure firewall application groups.
    edit <name>
        set application <id1>, <id2>, ...
        set behavior {user}
        set category <id1>, <id2>, ...
        set comment {var-string}
        set popularity {option1}, {option2}, ...
        set protocols {user}
        set risk <level1>, <level2>, ...
        set technology {user}
        set type [application|filter]
        set vendor {user}
    next
end

```

## config application group

Parameter	Description	Type	Size	Default
application <id>	Application ID list. Application IDs.	integer	Minimum value: 0 Maximum value: 4294967295	
behavior	Application behavior filter.	user	Not Specified	all

Parameter	Description	Type	Size	Default												
category <id>	Application category ID list. Category IDs.	integer	Minimum value: 0 Maximum value: 4294967295													
comment	Comments.	var-string	Maximum length: 255													
name	Application group name.	string	Maximum length: 63													
popularity	Application popularity filter.	option	-	1 2 3 4 5												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>1</td><td>Popularity level 1.</td></tr><tr><td>2</td><td>Popularity level 2.</td></tr><tr><td>3</td><td>Popularity level 3.</td></tr><tr><td>4</td><td>Popularity level 4.</td></tr><tr><td>5</td><td>Popularity level 5.</td></tr></table>				Option	Description	1	Popularity level 1.	2	Popularity level 2.	3	Popularity level 3.	4	Popularity level 4.	5	Popularity level 5.
Option	Description															
1	Popularity level 1.															
2	Popularity level 2.															
3	Popularity level 3.															
4	Popularity level 4.															
5	Popularity level 5.															
protocols	Application protocol filter.	user	Not Specified	all												
risk <level>	Risk, or impact, of allowing traffic from this application to occur (1 - 5; Low, Elevated, Medium, High, and Critical). Risk, or impact, of allowing traffic from this application to occur (1 - 5; Low, Elevated, Medium, High, and Critical).	integer	Minimum value: 0 Maximum value: 4294967295													
technology	Application technology filter.	user	Not Specified	all												
type	Application group type.	option	-	application												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>application</td><td>Application ID.</td></tr><tr><td>filter</td><td>Application filter.</td></tr></table>				Option	Description	application	Application ID.	filter	Application filter.						
Option	Description															
application	Application ID.															
filter	Application filter.															
vendor	Application vendor filter.	user	Not Specified	all												

## config application list

Configure application control lists.

```
config application list
    Description: Configure application control lists.
    edit <name>
```

```

set app-replacemsg [disable|enable]
set comment {var-string}
set control-default-network-services [disable|enable]
set deep-app-inspection [disable|enable]
config default-network-services
    Description: Default network service entries.
    edit <id>
        set port {integer}
        set services {option1}, {option2}, ...
        set violation-action [pass|monitor|...]
    next
end
set enforce-default-app-port [disable|enable]
config entries
    Description: Application list entries.
    edit <id>
        set risk <level1>, <level2>, ...
        set category <id1>, <id2>, ...
        set application <id1>, <id2>, ...
        set protocols {user}
        set vendor {user}
        set technology {user}
        set behavior {user}
        set popularity {option1}, {option2}, ...
        set exclusion <id1>, <id2>, ...
        config parameters
            Description: Application parameters.
            edit <id>
                config members
                    Description: Parameter tuple members.
                    edit <id>
                        set name {string}
                        set value {string}
                    next
                end
            next
        end
    next
end
set action [pass|block|...]
set log [disable|enable]
set log-packet [disable|enable]
set rate-count {integer}
set rate-duration {integer}
set rate-mode [periodical|continuous]
set rate-track [none|src-ip|...]
set session-ttl {integer}
set shaper {string}
set shaper-reverse {string}
set per-ip-shaper {string}
set quarantine [none|attacker]
set quarantine-expiry {user}
set quarantine-log [disable|enable]
next
end
set extended-log [enable|disable]
set force-inclusion-ssl-di-sigs [disable|enable]
set options {option1}, {option2}, ...

```

```

set other-application-action [pass|block]
set other-application-log [disable|enable]
set p2p-block-list {option1}, {option2}, ...
set replacemsg-group {string}
set unknown-application-action [pass|block]
set unknown-application-log [disable|enable]
next
end

```

## config application list

Parameter	Description	Type	Size	Default						
app-replacemsg	Enable/disable replacement messages for blocked applications.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable replacement messages for blocked applications.</td></tr><tr><td><i>enable</i></td><td>Enable replacement messages for blocked applications.</td></tr></table>	Option	Description	<i>disable</i>	Disable replacement messages for blocked applications.	<i>enable</i>	Enable replacement messages for blocked applications.			
Option	Description									
<i>disable</i>	Disable replacement messages for blocked applications.									
<i>enable</i>	Enable replacement messages for blocked applications.									
comment	Comments.	var-string	Maximum length: 255							
control-default-network-services	Enable/disable enforcement of protocols over selected ports.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable protocol enforcement over selected ports.</td></tr><tr><td><i>enable</i></td><td>Enable protocol enforcement over selected ports.</td></tr></table>	Option	Description	<i>disable</i>	Disable protocol enforcement over selected ports.	<i>enable</i>	Enable protocol enforcement over selected ports.			
Option	Description									
<i>disable</i>	Disable protocol enforcement over selected ports.									
<i>enable</i>	Enable protocol enforcement over selected ports.									
deep-app-inspection	Enable/disable deep application inspection.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable deep application inspection.</td></tr><tr><td><i>enable</i></td><td>Enable deep application inspection.</td></tr></table>	Option	Description	<i>disable</i>	Disable deep application inspection.	<i>enable</i>	Enable deep application inspection.			
Option	Description									
<i>disable</i>	Disable deep application inspection.									
<i>enable</i>	Enable deep application inspection.									
enforce-default-app-port	Enable/disable default application port enforcement for allowed applications.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable default application port enforcement.</td></tr><tr><td><i>enable</i></td><td>Enable default application port enforcement.</td></tr></table>	Option	Description	<i>disable</i>	Disable default application port enforcement.	<i>enable</i>	Enable default application port enforcement.			
Option	Description									
<i>disable</i>	Disable default application port enforcement.									
<i>enable</i>	Enable default application port enforcement.									

Parameter	Description	Type	Size	Default												
extended-log	Enable/disable extended logging.	option	-	disable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.									
	Option	Description														
	<i>enable</i>	Enable setting.														
<i>disable</i>	Disable setting.															
force-inclusion-ssl-di-sigs	Enable/disable forced inclusion of SSL deep inspection signatures.	option	-	disable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable forced inclusion of signatures which normally require SSL deep inspection.</td></tr><tr><td><i>enable</i></td><td>Enable forced inclusion of signatures which normally require SSL deep inspection.</td></tr></table>	Option	Description	<i>disable</i>	Disable forced inclusion of signatures which normally require SSL deep inspection.	<i>enable</i>	Enable forced inclusion of signatures which normally require SSL deep inspection.									
	Option	Description														
	<i>disable</i>	Disable forced inclusion of signatures which normally require SSL deep inspection.														
<i>enable</i>	Enable forced inclusion of signatures which normally require SSL deep inspection.															
name	List name.	string	Maximum length: 35													
options	Basic application protocol signatures allowed by default.	option	-	allow-dns												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow-dns</i></td><td>Allow DNS.</td></tr><tr><td><i>allow-icmp</i></td><td>Allow ICMP.</td></tr><tr><td><i>allow-http</i></td><td>Allow generic HTTP web browsing.</td></tr><tr><td><i>allow-ssl</i></td><td>Allow generic SSL communication.</td></tr><tr><td><i>allow-quic</i></td><td>Allow QUIC.</td></tr></table>	Option	Description	<i>allow-dns</i>	Allow DNS.	<i>allow-icmp</i>	Allow ICMP.	<i>allow-http</i>	Allow generic HTTP web browsing.	<i>allow-ssl</i>	Allow generic SSL communication.	<i>allow-quic</i>	Allow QUIC.			
	Option	Description														
	<i>allow-dns</i>	Allow DNS.														
	<i>allow-icmp</i>	Allow ICMP.														
	<i>allow-http</i>	Allow generic HTTP web browsing.														
	<i>allow-ssl</i>	Allow generic SSL communication.														
<i>allow-quic</i>	Allow QUIC.															
other-application-action	Action for other applications.	option	-	pass												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>pass</i></td><td>Allow sessions matching an application in this application list.</td></tr><tr><td><i>block</i></td><td>Block sessions matching an application in this application list.</td></tr></table>	Option	Description	<i>pass</i>	Allow sessions matching an application in this application list.	<i>block</i>	Block sessions matching an application in this application list.									
	Option	Description														
	<i>pass</i>	Allow sessions matching an application in this application list.														
<i>block</i>	Block sessions matching an application in this application list.															
other-application-log	Enable/disable logging for other applications.	option	-	disable												

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable logging for other applications.		
	<i>enable</i>	Enable logging for other applications.		
p2p-block-list	P2P applications to be block listed.	option	-	
	<b>Option</b>	<b>Description</b>		
	<i>skype</i>	Skype.		
	<i>edonkey</i>	Edonkey.		
	<i>bittorrent</i>	Bit torrent.		
replacemsg-group	Replacement message group.	string	Maximum length: 35	
unknown-application-action	Pass or block traffic from unknown applications.	option	-	pass
	<b>Option</b>	<b>Description</b>		
	<i>pass</i>	Pass or allow unknown applications.		
	<i>block</i>	Drop or block unknown applications.		
unknown-application-log	Enable/disable logging for unknown applications.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable logging for unknown applications.		
	<i>enable</i>	Enable logging for unknown applications.		

### config default-network-services

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
port	Port number.	integer	Minimum value: 0 Maximum value: 65535	0



Parameter	Description	Type	Size	Default																								
services	Network protocols.	option	-																									
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>http</i></td><td>HTTP.</td></tr><tr><td><i>ssh</i></td><td>SSH.</td></tr><tr><td><i>telnet</i></td><td>TELNET.</td></tr><tr><td><i>ftp</i></td><td>FTP.</td></tr><tr><td><i>dns</i></td><td>DNS.</td></tr><tr><td><i>smtp</i></td><td>SMTP.</td></tr><tr><td><i>pop3</i></td><td>POP3.</td></tr><tr><td><i>imap</i></td><td>IMAP.</td></tr><tr><td><i>snmp</i></td><td>SNMP.</td></tr><tr><td><i>nntp</i></td><td>NNTP.</td></tr><tr><td><i>https</i></td><td>HTTPS.</td></tr></table>	Option	Description	<i>http</i>	HTTP.	<i>ssh</i>	SSH.	<i>telnet</i>	TELNET.	<i>ftp</i>	FTP.	<i>dns</i>	DNS.	<i>smtp</i>	SMTP.	<i>pop3</i>	POP3.	<i>imap</i>	IMAP.	<i>snmp</i>	SNMP.	<i>nntp</i>	NNTP.	<i>https</i>	HTTPS.			
	Option	Description																										
	<i>http</i>	HTTP.																										
	<i>ssh</i>	SSH.																										
	<i>telnet</i>	TELNET.																										
	<i>ftp</i>	FTP.																										
	<i>dns</i>	DNS.																										
	<i>smtp</i>	SMTP.																										
	<i>pop3</i>	POP3.																										
	<i>imap</i>	IMAP.																										
	<i>snmp</i>	SNMP.																										
	<i>nntp</i>	NNTP.																										
<i>https</i>	HTTPS.																											
violation-action	Action for protocols not in the allowlist for selected port.	option	-	block																								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>pass</i></td><td>Allow protocols not in the allowlist for selected port.</td></tr><tr><td><i>monitor</i></td><td>Monitor protocols not in the allowlist for selected port.</td></tr><tr><td><i>block</i></td><td>Block protocols not in the allowlist for selected port.</td></tr></table>	Option	Description	<i>pass</i>	Allow protocols not in the allowlist for selected port.	<i>monitor</i>	Monitor protocols not in the allowlist for selected port.	<i>block</i>	Block protocols not in the allowlist for selected port.																			
	Option	Description																										
	<i>pass</i>	Allow protocols not in the allowlist for selected port.																										
	<i>monitor</i>	Monitor protocols not in the allowlist for selected port.																										
<i>block</i>	Block protocols not in the allowlist for selected port.																											

## config entries

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
risk <level>	<p>Risk, or impact, of allowing traffic from this application to occur (1 - 5; Low, Elevated, Medium, High, and Critical).</p> <p>Risk, or impact, of allowing traffic from this application to occur (1 - 5; Low, Elevated, Medium, High, and Critical).</p>	integer	Minimum value: 0 Maximum value: 4294967295	

Parameter	Description	Type	Size	Default												
category <id>	Category ID list. Application category ID.	integer	Minimum value: 0 Maximum value: 4294967295													
application <id>	ID of allowed applications. Application IDs.	integer	Minimum value: 0 Maximum value: 4294967295													
protocols	Application protocol filter.	user	Not Specified	all												
vendor	Application vendor filter.	user	Not Specified	all												
technology	Application technology filter.	user	Not Specified	all												
behavior	Application behavior filter.	user	Not Specified	all												
popularity	Application popularity filter.	option	-	1 2 3 4 5												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>1</td><td>Popularity level 1.</td></tr><tr><td>2</td><td>Popularity level 2.</td></tr><tr><td>3</td><td>Popularity level 3.</td></tr><tr><td>4</td><td>Popularity level 4.</td></tr><tr><td>5</td><td>Popularity level 5.</td></tr></table>				Option	Description	1	Popularity level 1.	2	Popularity level 2.	3	Popularity level 3.	4	Popularity level 4.	5	Popularity level 5.
Option	Description															
1	Popularity level 1.															
2	Popularity level 2.															
3	Popularity level 3.															
4	Popularity level 4.															
5	Popularity level 5.															
exclusion <id>	ID of excluded applications. Excluded application IDs.	integer	Minimum value: 0 Maximum value: 4294967295													
action	Pass or block traffic, or reset connection for traffic from this application.	option	-	block												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>pass</td><td>Pass or allow matching traffic.</td></tr><tr><td>block</td><td>Block or drop matching traffic.</td></tr><tr><td>reset</td><td>Reset sessions for matching traffic.</td></tr></table>				Option	Description	pass	Pass or allow matching traffic.	block	Block or drop matching traffic.	reset	Reset sessions for matching traffic.				
Option	Description															
pass	Pass or allow matching traffic.															
block	Block or drop matching traffic.															
reset	Reset sessions for matching traffic.															
log	Enable/disable logging for this application list.	option	-	enable												

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable logging.		
	<i>enable</i>	Enable logging.		
log-packet	Enable/disable packet logging.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable packet logging.		
	<i>enable</i>	Enable packet logging.		
rate-count	Count of the rate.	integer	Minimum value: 0 Maximum value: 65535	0
rate-duration	Duration (sec) of the rate.	integer	Minimum value: 1 Maximum value: 65535	60
rate-mode	Rate limit mode.	option	-	continuous
	<b>Option</b>	<b>Description</b>		
	<i>periodical</i>	Allow configured number of packets every rate-duration.		
	<i>continuous</i>	Block packets once the rate is reached.		
rate-track	Track the packet protocol field.	option	-	none
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	none		
	<i>src-ip</i>	Source IP.		
	<i>dest-ip</i>	Destination IP.		
	<i>dhcp-client-mac</i>	DHCP client.		
	<i>dns-domain</i>	DNS domain.		
session-ttl	Session TTL.	integer	Minimum value: 0 Maximum value: 4294967295	0

Parameter	Description	Type	Size	Default						
shaper	Traffic shaper.	string	Maximum length: 35							
shaper-reverse	Reverse traffic shaper.	string	Maximum length: 35							
per-ip-shaper	Per-IP traffic shaper.	string	Maximum length: 35							
quarantine	Quarantine method.	option	-	none						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>Quarantine is disabled.</td></tr><tr><td><i>attacker</i></td><td>Block all traffic sent from attacker's IP address. The attacker's IP address is also added to the banned user list. The target's address is not affected.</td></tr></table>				Option	Description	<i>none</i>	Quarantine is disabled.	<i>attacker</i>	Block all traffic sent from attacker's IP address. The attacker's IP address is also added to the banned user list. The target's address is not affected.
	Option	Description								
	<i>none</i>	Quarantine is disabled.								
<i>attacker</i>	Block all traffic sent from attacker's IP address. The attacker's IP address is also added to the banned user list. The target's address is not affected.									
quarantine-expiry	Duration of quarantine.. Requires quarantine set to attacker.	user	Not Specified	5m						
quarantine-log	Enable/disable quarantine logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable quarantine logging.</td></tr><tr><td><i>enable</i></td><td>Enable quarantine logging.</td></tr></table>				Option	Description	<i>disable</i>	Disable quarantine logging.	<i>enable</i>	Enable quarantine logging.
	Option	Description								
	<i>disable</i>	Disable quarantine logging.								
<i>enable</i>	Enable quarantine logging.									

### config parameters

Parameter	Description	Type	Size	Default
id	Parameter tuple ID.	integer	Minimum value: 0 Maximum value: 4294967295	0

### config members

Parameter	Description	Type	Size	Default
id	Parameter.	integer	Minimum value: 0 Maximum value: 4294967295	0

Parameter	Description	Type	Size	Default
name	Parameter name.	string	Maximum length: 31	
value	Parameter value.	string	Maximum length: 199	

## config application name

Configure application signatures.

```

config application name
    Description: Configure application signatures.
    edit <name>
        set behavior {user}
        set category {integer}
        set id {integer}
        config metadata
            Description: Meta data.
            edit <id>
                set metaid {integer}
                set valueid {integer}
            next
        end
    config parameters
        Description: Application parameters.
        edit <name>
            set default value {string}
        next
    end
    set popularity {integer}
    set protocol {user}
    set risk {integer}
    set technology {user}
    set vendor {user}
    set weight {integer}
next
end

```

## config application name

Parameter	Description	Type	Size	Default
behavior	Application behavior.	user	Not Specified	
category	Application category ID.	integer	Minimum value: 0 Maximum value: 4294967295	0

Parameter	Description	Type	Size	Default
id	Application ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
name	Application name.	string	Maximum length: 63	
popularity	Application popularity.	integer	Minimum value: 0 Maximum value: 255	0
protocol	Application protocol.	user	Not Specified	
risk	Application risk.	integer	Minimum value: 0 Maximum value: 255	0
technology	Application technology.	user	Not Specified	
vendor	Application vendor.	user	Not Specified	
weight	Application weight.	integer	Minimum value: 0 Maximum value: 255	0

### config metadata

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
metaid	Meta ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
valueid	Value ID.	integer	Minimum value: 0 Maximum value: 4294967295	0

## config parameters

Parameter	Description	Type	Size	Default
name	Parameter name.	string	Maximum length: 31	
default value	Parameter default value.	string	Maximum length: 199	

## config application rule-settings

Configure application rule settings.

```
config application rule-settings
    Description: Configure application rule settings.
    edit <id>
        next
    end
```

## config application rule-settings

Parameter	Description	Type	Size	Default
id	Rule ID.	integer	Minimum value: 0 Maximum value: 4294967295	0

## authentication

This section includes syntax for the following commands:

- [config authentication rule on page 76](#)
- [config authentication scheme on page 78](#)
- [config authentication setting on page 80](#)

### config authentication rule

Configure Authentication Rules.

```
config authentication rule
  Description: Configure Authentication Rules.
  edit <name>
    set active-auth-method {string}
    set comments {var-string}
    set dstaddr <name1>, <name2>, ...
    set dstaddr6 <name1>, <name2>, ...
    set ip-based [enable|disable]
    set protocol [http|ftp|...]
    set srcaddr <name1>, <name2>, ...
    set srcaddr6 <name1>, <name2>, ...
    set srcintf <name1>, <name2>, ...
    set sso-auth-method {string}
    set status [enable|disable]
    set transaction-based [enable|disable]
    set web-auth-cookie [enable|disable]
    set web-portal [enable|disable]
  next
end
```

### config authentication rule

Parameter	Description	Type	Size	Default
active-auth-method	Select an active authentication method.	string	Maximum length: 35	
comments	Comment.	var-string	Maximum length: 1023	
dstaddr <name>	Select an IPv4 destination address from available options. Required for web proxy authentication. Address name.	string	Maximum length: 79	
dstaddr6 <name>	Select an IPv6 destination address from available options. Required for web proxy authentication.	string	Maximum length: 79	



Parameter	Description	Type	Size	Default										
	Address name.													
ip-based	Enable/disable IP-based authentication. When enabled, previously authenticated users from the same IP address will be exempted.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable IP-based authentication.</td></tr><tr><td><i>disable</i></td><td>Disable IP-based authentication.</td></tr></table>	Option	Description	<i>enable</i>	Enable IP-based authentication.	<i>disable</i>	Disable IP-based authentication.							
Option	Description													
<i>enable</i>	Enable IP-based authentication.													
<i>disable</i>	Disable IP-based authentication.													
name	Authentication rule name.	string	Maximum length: 35											
protocol	Authentication is required for the selected protocol.	option	-	http										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>http</i></td><td>HTTP traffic is matched and authentication is required.</td></tr><tr><td><i>ftp</i></td><td>FTP traffic is matched and authentication is required.</td></tr><tr><td><i>socks</i></td><td>SOCKS traffic is matched and authentication is required.</td></tr><tr><td><i>ssh</i></td><td>SSH traffic is matched and authentication is required.</td></tr></table>	Option	Description	<i>http</i>	HTTP traffic is matched and authentication is required.	<i>ftp</i>	FTP traffic is matched and authentication is required.	<i>socks</i>	SOCKS traffic is matched and authentication is required.	<i>ssh</i>	SSH traffic is matched and authentication is required.			
Option	Description													
<i>http</i>	HTTP traffic is matched and authentication is required.													
<i>ftp</i>	FTP traffic is matched and authentication is required.													
<i>socks</i>	SOCKS traffic is matched and authentication is required.													
<i>ssh</i>	SSH traffic is matched and authentication is required.													
srcaddr <name>	Authentication is required for the selected IPv4 source address. Address name.	string	Maximum length: 79											
srcaddr6 <name>	Authentication is required for the selected IPv6 source address. Address name.	string	Maximum length: 79											
srcintf <name>	Incoming (ingress) interface. Interface name.	string	Maximum length: 79											
sso-auth-method	Select a single-sign on (SSO) authentication method.	string	Maximum length: 35											
status	Enable/disable this authentication rule.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable this authentication rule.</td></tr><tr><td><i>disable</i></td><td>Disable this authentication rule.</td></tr></table>	Option	Description	<i>enable</i>	Enable this authentication rule.	<i>disable</i>	Disable this authentication rule.							
Option	Description													
<i>enable</i>	Enable this authentication rule.													
<i>disable</i>	Disable this authentication rule.													
transaction-based	Enable/disable transaction based authentication.	option	-	disable										

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable transaction based authentication.		
	<i>disable</i>	Disable transaction based authentication.		
web-auth-cookie	Enable/disable Web authentication cookies.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable Web authentication cookie.		
	<i>disable</i>	Disable Web authentication cookie.		
web-portal	Enable/disable web portal for proxy transparent policy.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable web-portal.		
	<i>disable</i>	Disable web-portal.		

## config authentication scheme

Configure Authentication Schemes.

```

config authentication scheme
    Description: Configure Authentication Schemes.
    edit <name>
        set domain-controller {string}
        set fsso-agent-for-ntlm {string}
        set fsso-guest [enable|disable]
        set kerberos-keytab {string}
        set method {option1}, {option2}, ...
        set negotiate-ntlm [enable|disable]
        set require-tfa [enable|disable]
        set saml-server {string}
        set saml-timeout {integer}
        set ssh-ca {string}
        set user-cert [enable|disable]
        set user-database <name1>, <name2>, ...
    next
end

```

## config authentication scheme

Parameter	Description	Type	Size	Default
domain-controller	Domain controller setting.	string	Maximum length: 35	

Parameter	Description	Type	Size	Default
fsso-agent-for-ntlm	FSSO agent to use for NTLM authentication.	string	Maximum length: 35	
fsso-guest	Enable/disable user fsso-guest authentication.	option	-	disable
	Option	Description		
	enable	Enable user fsso-guest authentication.		
	disable	Disable user fsso-guest authentication.		
kerberos-keytab	Kerberos keytab setting.	string	Maximum length: 35	
method	Authentication methods.	option	-	
	Option	Description		
	ntlm	NTLM authentication.		
	basic	Basic HTTP authentication.		
	digest	Digest HTTP authentication.		
	form	Form-based HTTP authentication.		
	negotiate	Negotiate authentication.		
	fsso	Fortinet Single Sign-On (FSSO) authentication.		
	rssso	RADIUS Single Sign-On (RSSO) authentication.		
	ssh-publickey	Public key based SSH authentication.		
	cert	Client certificate authentication.		
	saml	SAML authentication.		
name	Authentication scheme name.	string	Maximum length: 35	
negotiate-ntlm	Enable/disable negotiate authentication for NTLM.	option	-	enable
	Option	Description		
	enable	Enable negotiate authentication for NTLM.		
	disable	Disable negotiate authentication for NTLM.		
require-tfa	Enable/disable two-factor authentication.	option	-	disable
	Option	Description		
	enable	Enable two-factor authentication.		

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable two-factor authentication.</td></tr></table>				Option	Description	<i>disable</i>	Disable two-factor authentication.		
Option	Description									
<i>disable</i>	Disable two-factor authentication.									
saml-server	SAML configuration.	string	Maximum length: 35							
saml-timeout	SAML authentication timeout in seconds.	integer	Minimum value: 30 Maximum value: 1200	120						
ssh-ca	SSH CA name.	string	Maximum length: 35							
user-cert	Enable/disable authentication with user certificate.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable client certificate field authentication.</td></tr><tr><td><i>disable</i></td><td>Disable client certificate field authentication.</td></tr></table>				Option	Description	<i>enable</i>	Enable client certificate field authentication.	<i>disable</i>	Disable client certificate field authentication.
Option	Description									
<i>enable</i>	Enable client certificate field authentication.									
<i>disable</i>	Disable client certificate field authentication.									
user-database <name>	Authentication server to contain user information; "local" (default) or "123" (for LDAP). Authentication server name.	string	Maximum length: 79							

## config authentication setting

Configure authentication setting.

```

config authentication setting
    Description: Configure authentication setting.
    set active-auth-scheme {string}
    set auth-https [enable|disable]
    set captive-portal {string}
    set captive-portal-ip {ipv4-address-any}
    set captive-portal-ip6 {ipv6-address}
    set captive-portal-port {integer}
    set captive-portal-ssl-port {integer}
    set captive-portal-type [fqdn|ip]
    set captive-portal6 {string}
    set cert-auth [enable|disable]
    set cert-captive-portal {string}
    set cert-captive-portal-ip {ipv4-address-any}
    set cert-captive-portal-port {integer}
    set dev-range <name1>, <name2>, ...
    set sso-auth-scheme {string}
    set user-cert-ca <name1>, <name2>, ...
end

```

## config authentication setting

Parameter	Description	Type	Size	Default
active-auth-scheme	Active authentication method (scheme name).	string	Maximum length: 35	
auth-https	Enable/disable redirecting HTTP user authentication to HTTPS.	option	-	enable
	Option	Description		
	enable	Enable setting.		
	disable	Disable setting.		
captive-portal	Captive portal host name.	string	Maximum length: 255	
captive-portal-ip	Captive portal IP address.	ipv4-address-any	Not Specified	0.0.0.0
captive-portal-ip6	Captive portal IPv6 address.	ipv6-address	Not Specified	::
captive-portal-port	Captive portal port number.	integer	Minimum value: 1 Maximum value: 65535	7830
captive-portal-ssl-port	Captive portal SSL port number.	integer	Minimum value: 1 Maximum value: 65535	7831
captive-portal-type	Captive portal type.	option	-	fqdn
	Option	Description		
	fqdn	Use FQDN for captive portal.		
	ip	Use an IP address for captive portal.		
captive-portal6	IPv6 captive portal host name.	string	Maximum length: 255	
cert-auth	Enable/disable redirecting certificate authentication to HTTPS portal.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	enable	Enable setting.		
	disable	Disable setting.		
cert-captive-portal	Certificate captive portal host name.	string	Maximum length: 255	
cert-captive-portal-ip	Certificate captive portal IP address.	ipv4-address-any	Not Specified	0.0.0.0
cert-captive-portal-port	Certificate captive portal port number.	integer	Minimum value: 1 Maximum value: 65535	7832
dev-range <name>	Address range for the IP based device query. Address name.	string	Maximum length: 79	
sso-auth-scheme	Single-Sign-On authentication method (scheme name).	string	Maximum length: 35	
user-cert-ca <name>	CA certificate used for client certificate verification. CA certificate list.	string	Maximum length: 79	**

\*\* Values may differ between models.

## certificate

This section includes syntax for the following commands:

- [config certificate ca on page 83](#)
- [config certificate crl on page 84](#)
- [config certificate local on page 86](#)
- [config certificate remote on page 89](#)

### config certificate ca

CA certificate.

```
config certificate ca
  Description: CA certificate.
  edit <name>
    set auto-update-days {integer}
    set auto-update-days-warning {integer}
    set ca {user}
    set ca-identifier {string}
    set range [global|vdom]
    set scep-url {string}
    set source [factory|user|...]
    set source-ip {ipv4-address}
    set ssl-inspection-trusted [enable|disable]
  next
end
```

### config certificate ca

Parameter	Description	Type	Size	Default
auto-update-days	Number of days to wait before requesting an updated CA certificate.	integer	Minimum value: 0 Maximum value: 4294967295	0
auto-update-days-warning	Number of days before an expiry-warning message is generated.	integer	Minimum value: 0 Maximum value: 4294967295	0
ca	CA certificate as a PEM file.	user	Not Specified	

Parameter	Description	Type	Size	Default								
ca-identifier	CA identifier of the SCEP server.	string	Maximum length: 255									
name	Name.	string	Maximum length: 79									
range	Either global or VDOM IP address range for the CA certificate.	option	-	global								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>global</i></td><td>Global range.</td></tr><tr><td><i>vdom</i></td><td>VDOM IP address range.</td></tr></table>	Option	Description	<i>global</i>	Global range.	<i>vdom</i>	VDOM IP address range.					
Option	Description											
<i>global</i>	Global range.											
<i>vdom</i>	VDOM IP address range.											
scep-url	URL of the SCEP server.	string	Maximum length: 255									
source	CA certificate source type.	option	-	user								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>factory</i></td><td>Factory installed certificate.</td></tr><tr><td><i>user</i></td><td>User generated certificate.</td></tr><tr><td><i>bundle</i></td><td>Bundle file certificate.</td></tr></table>	Option	Description	<i>factory</i>	Factory installed certificate.	<i>user</i>	User generated certificate.	<i>bundle</i>	Bundle file certificate.			
Option	Description											
<i>factory</i>	Factory installed certificate.											
<i>user</i>	User generated certificate.											
<i>bundle</i>	Bundle file certificate.											
source-ip	Source IP address for communications to the SCEP server.	ipv4-address	Not Specified	0.0.0.0								
ssl-inspection-trusted	Enable/disable this CA as a trusted CA for SSL inspection.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Trusted CA for SSL inspection.</td></tr><tr><td><i>disable</i></td><td>Untrusted CA for SSL inspection.</td></tr></table>	Option	Description	<i>enable</i>	Trusted CA for SSL inspection.	<i>disable</i>	Untrusted CA for SSL inspection.					
Option	Description											
<i>enable</i>	Trusted CA for SSL inspection.											
<i>disable</i>	Untrusted CA for SSL inspection.											

## config certificate crl

Certificate Revocation List as a PEM file.

```
config certificate crl
  Description: Certificate Revocation List as a PEM file.
  edit <name>
    set crl {user}
    set http-url {string}
    set ldap-password {password}
    set ldap-server {string}
    set ldap-username {string}
```



```

        set range [global|vdom]
        set scep-cert {string}
        set scep-url {string}
        set source [factory|user|...]
        set source-ip {ipv4-address}
        set update-interval {integer}
        set update-vdom {string}
    next
end

```

## config certificate crl

Parameter	Description	Type	Size	Default								
crl	Certificate Revocation List as a PEM file.	user	Not Specified									
http-url	HTTP server URL for CRL auto-update.	string	Maximum length: 255									
ldap-password	LDAP server user password.	password	Not Specified									
ldap-server	LDAP server name for CRL auto-update.	string	Maximum length: 35									
ldap-username	LDAP server user name.	string	Maximum length: 63									
name	Name.	string	Maximum length: 35									
range	Either global or VDOM IP address range for the certificate.	option	-	global								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>global</i></td><td>Global range.</td></tr><tr><td><i>vdom</i></td><td>VDOM IP address range.</td></tr></table>				Option	Description	<i>global</i>	Global range.	<i>vdom</i>	VDOM IP address range.		
Option	Description											
<i>global</i>	Global range.											
<i>vdom</i>	VDOM IP address range.											
scep-cert	Local certificate for SCEP communication for CRL auto-update.	string	Maximum length: 35	Fortinet_CA_SSL								
scep-url	SCEP server URL for CRL auto-update.	string	Maximum length: 255									
source	Certificate source type.	option	-	user								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>factory</i></td><td>Factory installed certificate.</td></tr><tr><td><i>user</i></td><td>User generated certificate.</td></tr><tr><td><i>bundle</i></td><td>Bundle file certificate.</td></tr></table>				Option	Description	<i>factory</i>	Factory installed certificate.	<i>user</i>	User generated certificate.	<i>bundle</i>	Bundle file certificate.
Option	Description											
<i>factory</i>	Factory installed certificate.											
<i>user</i>	User generated certificate.											
<i>bundle</i>	Bundle file certificate.											

Parameter	Description	Type	Size	Default
source-ip	Source IP address for communications to a HTTP or SCEP CA server.	ipv4-address	Not Specified	0.0.0.0
update-interval	Time in seconds before the FortiGate checks for an updated CRL. Set to 0 to update only when it expires.	integer	Minimum value: 0 Maximum value: 4294967295	0
update-vdom	VDOM for CRL update.	string	Maximum length: 31	root

## config certificate local

Local keys and certificates.

```

config certificate local
    Description: Local keys and certificates.
    edit <name>
        set acme-ca-url {string}
        set acme-domain {string}
        set acme-email {string}
        set acme-renew-window {integer}
        set acme-rsa-key-size {integer}
        set auto-regenerate-days {integer}
        set auto-regenerate-days-warning {integer}
        set ca-identifier {string}
        set certificate {user}
        set cmp-path {string}
        set cmp-regeneration-method [keyupdate|renewal]
        set cmp-server {string}
        set cmp-server-cert {string}
        set comments {string}
        set csr {user}
        set enroll-protocol [none|scep|...]
        set ike-localid {string}
        set ike-localid-type [asn1dn|fqdn]
        set name-encoding [printable|utf8]
        set password {password}
        set private-key {user}
        set range [global|vdom]
        set scep-password {password}
        set scep-url {string}
        set source [factory|user|...]
        set source-ip {ipv4-address}
        set state {user}
    next
end

```

## config certificate local

Parameter	Description	Type	Size	Default
acme-ca-url	The URL for the ACME CA server.	string	Maximum length: 255	https://acme-v02.api.letsencrypt.org/directory
acme-domain	A valid domain that resolves to this FortiGate unit.	string	Maximum length: 255	
acme-email	Contact email address that is required by some CAs like LetsEncrypt.	string	Maximum length: 255	
acme-renew-window	Beginning of the renewal window.	integer	Minimum value: 1 Maximum value: 100	30
acme-rsa-key-size	Length of the RSA private key of the generated cert (Minimum 2048 bits).	integer	Minimum value: 2048 Maximum value: 4096	2048
auto-regenerate-days	Number of days to wait before expiry of an updated local certificate is requested (0 = disabled).	integer	Minimum value: 0 Maximum value: 4294967295	0
auto-regenerate-days-warning	Number of days to wait before an expiry warning message is generated (0 = disabled).	integer	Minimum value: 0 Maximum value: 4294967295	0
ca-identifier	CA identifier of the CA server for signing via SCEP.	string	Maximum length: 255	
certificate	PEM format certificate.	user	Not Specified	
cmp-path	Path location inside CMP server.	string	Maximum length: 255	
cmp-regeneration-method	CMP auto-regeneration method.	option	-	keyupate
		Option	Description	
		<i>keyupate</i>	Key Update.	
		<i>renewal</i>	Renewal.	

Parameter	Description	Type	Size	Default										
cmp-server	Address and port for CMP server (format = address:port).	string	Maximum length: 63											
cmp-server-cert	CMP server certificate.	string	Maximum length: 79											
comments	Comment.	string	Maximum length: 511											
csr	Certificate Signing Request.	user	Not Specified											
enroll-protocol	Certificate enrollment protocol.	option	-	none										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>None (default).</td></tr><tr><td><i>scep</i></td><td>Simple Certificate Enrollment Protocol.</td></tr><tr><td><i>cmpv2</i></td><td>Certificate Management Protocol Version 2.</td></tr><tr><td><i>acme2</i></td><td>Automated Certificate Management Environment Version 2.</td></tr></table>				Option	Description	<i>none</i>	None (default).	<i>scep</i>	Simple Certificate Enrollment Protocol.	<i>cmpv2</i>	Certificate Management Protocol Version 2.	<i>acme2</i>	Automated Certificate Management Environment Version 2.
Option	Description													
<i>none</i>	None (default).													
<i>scep</i>	Simple Certificate Enrollment Protocol.													
<i>cmpv2</i>	Certificate Management Protocol Version 2.													
<i>acme2</i>	Automated Certificate Management Environment Version 2.													
ike-localid	Local ID the FortiGate uses for authentication as a VPN client.	string	Maximum length: 63											
ike-localid-type	IKE local ID type.	option	-	asn1dn										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>asn1dn</i></td><td>ASN.1 distinguished name.</td></tr><tr><td><i>fqdn</i></td><td>Fully qualified domain name.</td></tr></table>				Option	Description	<i>asn1dn</i>	ASN.1 distinguished name.	<i>fqdn</i>	Fully qualified domain name.				
Option	Description													
<i>asn1dn</i>	ASN.1 distinguished name.													
<i>fqdn</i>	Fully qualified domain name.													
name	Name.	string	Maximum length: 35											
name-encoding	Name encoding method for auto-regeneration.	option	-	printable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>printable</i></td><td>Printable encoding (default).</td></tr><tr><td><i>utf8</i></td><td>UTF-8 encoding.</td></tr></table>				Option	Description	<i>printable</i>	Printable encoding (default).	<i>utf8</i>	UTF-8 encoding.				
Option	Description													
<i>printable</i>	Printable encoding (default).													
<i>utf8</i>	UTF-8 encoding.													
password	Password as a PEM file.	password	Not Specified											
private-key	PEM format key encrypted with a password.	user	Not Specified											

Parameter	Description	Type	Size	Default
range	Either a global or VDOM IP address range for the certificate.	option	-	global
	<b>Option</b>	<b>Description</b>		
	<i>global</i>	Global range.		
	<i>vdom</i>	VDOM IP address range.		
scep-password	SCEP server challenge password for auto-regeneration.	password	Not Specified	
scep-url	SCEP server URL.	string	Maximum length: 255	
source	Certificate source type.	option	-	user
	<b>Option</b>	<b>Description</b>		
	<i>factory</i>	Factory installed certificate.		
	<i>user</i>	User generated certificate.		
	<i>bundle</i>	Bundle file certificate.		
source-ip	Source IP address for communications to the SCEP server.	ipv4-address	Not Specified	0.0.0.0
state	Certificate Signing Request State.	user	Not Specified	

## config certificate remote

Remote certificate as a PEM file.

```

config certificate remote
    Description: Remote certificate as a PEM file.
    edit <name>
        set range [global|vdom]
        set remote {user}
        set source [factory|user|...]
    next
end

```

## config certificate remote

Parameter	Description	Type	Size	Default
name	Name.	string	Maximum length: 35	
range	Either the global or VDOM IP address range for the remote certificate.	option	-	global
	Option	Description		
	global	Global range.		
	vdom	VDOM IP address range.		
remote	Remote certificate.	user	Not Specified	
source	Remote certificate source type.	option	-	user
	Option	Description		
	factory	Factory installed certificate.		
	user	User generated certificate.		
	bundle	Bundle file certificate.		

## dlp

This section includes syntax for the following commands:

- [config dlp filepattern on page 91](#)
- [config dlp fp-doc-source on page 94](#)
- [config dlp sensitivity on page 97](#)
- [config dlp sensor on page 98](#)
- [config dlp settings on page 103](#)

### config dlp filepattern

Configure file patterns used by DLP blocking.

```
config dlp filepattern
  Description: Configure file patterns used by DLP blocking.
  edit <id>
    set comment {var-string}
    config entries
      Description: Configure file patterns used by DLP blocking.
      edit <pattern>
        set filter-type [pattern|type]
        set file-type [7z|arj|...]
      next
    end
    set name {string}
  next
end
```

### config dlp filepattern

Parameter	Description	Type	Size	Default
comment	Optional comments.	var-string	Maximum length: 255	
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
name	Name of table containing the file pattern list.	string	Maximum length: 63	

## config entries

Parameter	Description	Type	Size	Default																																												
filter-type	Filter by file name pattern or by file type.	option	-	pattern																																												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>pattern</i></td><td>Filter by file name pattern.</td></tr><tr><td><i>type</i></td><td>Filter by file type.</td></tr></table>				Option	Description	<i>pattern</i>	Filter by file name pattern.	<i>type</i>	Filter by file type.																																						
	Option	Description																																														
	<i>pattern</i>	Filter by file name pattern.																																														
<i>type</i>	Filter by file type.																																															
pattern	Add a file name pattern.	string	Maximum length: 79																																													
file-type	Select a file type.	option	-	unknown																																												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>7z</i></td><td>Match 7-zip files.</td></tr><tr><td><i>arj</i></td><td>Match arj compressed files.</td></tr><tr><td><i>cab</i></td><td>Match Windows cab files.</td></tr><tr><td><i>lzh</i></td><td>Match lzh compressed files.</td></tr><tr><td><i>rar</i></td><td>Match rar archives.</td></tr><tr><td><i>tar</i></td><td>Match tar files.</td></tr><tr><td><i>zip</i></td><td>Match zip files.</td></tr><tr><td><i>bzip</i></td><td>Match bzip files.</td></tr><tr><td><i>gzip</i></td><td>Match gzip files.</td></tr><tr><td><i>bzip2</i></td><td>Match bzip2 files.</td></tr><tr><td><i>xz</i></td><td>Match xz files.</td></tr><tr><td><i>bat</i></td><td>Match Windows batch files.</td></tr><tr><td><i>uue</i></td><td>Match uue files.</td></tr><tr><td><i>mime</i></td><td>Match mime files.</td></tr><tr><td><i>base64</i></td><td>Match base64 files.</td></tr><tr><td><i>binhex</i></td><td>Match binhex files.</td></tr><tr><td><i>elf</i></td><td>Match elf files.</td></tr><tr><td><i>exe</i></td><td>Match Windows executable files.</td></tr><tr><td><i>hta</i></td><td>Match hta files.</td></tr><tr><td><i>html</i></td><td>Match html files.</td></tr><tr><td><i>jad</i></td><td>Match jad files.</td></tr></table>				Option	Description	<i>7z</i>	Match 7-zip files.	<i>arj</i>	Match arj compressed files.	<i>cab</i>	Match Windows cab files.	<i>lzh</i>	Match lzh compressed files.	<i>rar</i>	Match rar archives.	<i>tar</i>	Match tar files.	<i>zip</i>	Match zip files.	<i>bzip</i>	Match bzip files.	<i>gzip</i>	Match gzip files.	<i>bzip2</i>	Match bzip2 files.	<i>xz</i>	Match xz files.	<i>bat</i>	Match Windows batch files.	<i>uue</i>	Match uue files.	<i>mime</i>	Match mime files.	<i>base64</i>	Match base64 files.	<i>binhex</i>	Match binhex files.	<i>elf</i>	Match elf files.	<i>exe</i>	Match Windows executable files.	<i>hta</i>	Match hta files.	<i>html</i>	Match html files.	<i>jad</i>	Match jad files.
	Option	Description																																														
	<i>7z</i>	Match 7-zip files.																																														
	<i>arj</i>	Match arj compressed files.																																														
	<i>cab</i>	Match Windows cab files.																																														
	<i>lzh</i>	Match lzh compressed files.																																														
	<i>rar</i>	Match rar archives.																																														
	<i>tar</i>	Match tar files.																																														
	<i>zip</i>	Match zip files.																																														
	<i>bzip</i>	Match bzip files.																																														
	<i>gzip</i>	Match gzip files.																																														
	<i>bzip2</i>	Match bzip2 files.																																														
	<i>xz</i>	Match xz files.																																														
	<i>bat</i>	Match Windows batch files.																																														
	<i>uue</i>	Match uue files.																																														
	<i>mime</i>	Match mime files.																																														
	<i>base64</i>	Match base64 files.																																														
	<i>binhex</i>	Match binhex files.																																														
	<i>elf</i>	Match elf files.																																														
	<i>exe</i>	Match Windows executable files.																																														
	<i>hta</i>	Match hta files.																																														
<i>html</i>	Match html files.																																															
<i>jad</i>	Match jad files.																																															



Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>class</i>	Match class files.		
	<i>cod</i>	Match cod files.		
	<i>javascript</i>	Match javascript files.		
	<i>msoffice</i>	Match MS-Office files. For example, doc, xls, ppt, and so on.		
	<i>msofficex</i>	Match MS-Office XML files. For example, docx, xlsx, pptx, and so on.		
	<i>fsg</i>	Match fsg files.		
	<i>upx</i>	Match upx files.		
	<i>petite</i>	Match petite files.		
	<i>aspack</i>	Match aspack files.		
	<i>sis</i>	Match sis files.		
	<i>hlp</i>	Match Windows help files.		
	<i>activemime</i>	Match activemime files.		
	<i>jpeg</i>	Match jpeg files.		
	<i>gif</i>	Match gif files.		
	<i>tiff</i>	Match tiff files.		
	<i>png</i>	Match png files.		
	<i>bmp</i>	Match bmp files.		
	<i>unknown</i>	Match unknown files.		
	<i>mpeg</i>	Match mpeg files.		
	<i>mov</i>	Match mov files.		
	<i>mp3</i>	Match mp3 files.		
	<i>wma</i>	Match wma files.		
	<i>wav</i>	Match wav files.		
	<i>pdf</i>	Match Acrobat PDF files.		
	<i>avi</i>	Match avi files.		
	<i>rm</i>	Match rm files.		
	<i>torrent</i>	Match torrent files.		
	<i>hibun</i>	Match special-file-23-support files.		
	<i>msi</i>	Match Windows Installer msi files.		

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>mach-o</i>	Match Mach object files.		
	<i>dmg</i>	Match Apple disk image files.		
	<i>.net</i>	Match .NET files.		
	<i>xar</i>	Match xar archive files.		
	<i>chm</i>	Match Windows compiled HTML help files.		
	<i>iso</i>	Match ISO archive files.		
	<i>crx</i>	Match Chrome extension files.		
	<i>flac</i>	Match flac files.		

## config dlp fp-doc-source



This command is available for model(s): FortiGate 1000D, FortiGate 101E, FortiGate 101F, FortiGate 1101E, FortiGate 1200D, FortiGate 1500DT, FortiGate 1500D, FortiGate 1801F, FortiGate 2000E, FortiGate 201E, FortiGate 201F, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3001F, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3301E, FortiGate 3401E, FortiGate 3501F, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4201F, FortiGate 4401F, FortiGate 5001E1, FortiGate 501E, FortiGate 601E, FortiGate 601F, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 91E, FortiGate VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 1100E, FortiGate 140E-POE, FortiGate 140E, FortiGate 1800F, FortiGate 200E, FortiGate 200F, FortiGate 2200E, FortiGate 3000F, FortiGate 300E, FortiGate 3300E, FortiGate 3400E, FortiGate 3500F, FortiGate 3600E, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 4200F, FortiGate 4400F, FortiGate 5001E, FortiGate 500E, FortiGate 600E, FortiGate 600F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F-POE, FortiGate 80F, FortiGate 90E, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E.

Create a DLP fingerprint database by allowing the FortiGate to access a file server containing files from which to create fingerprints.

```
config dlp fp-doc-source
```

```
    Description: Create a DLP fingerprint database by allowing the FortiGate to access a
    file server containing files from which to create fingerprints.
```

```
    edit <name>
```

```
        set date {integer}
```

```

set file-path {string}
set file-pattern {string}
set keep-modified [enable|disable]
set password {password}
set period [none|daily|...]
set remove-deleted [enable|disable]
set scan-on-creation [enable|disable]
set scan-subdirectories [enable|disable]
set sensitivity {string}
set server {string}
set server-type {option}
set tod-hour {integer}
set tod-min {integer}
set username {string}
set vdom [mgmt|current]
set weekday [sunday|monday|...]

```

```

next

```

```

end

```

## config dlp fp-doc-source

Parameter	Description	Type	Size	Default						
date	Day of the month on which to scan the server.	integer	Minimum value: 1 Maximum value: 31	1						
file-path	Path on the server to the fingerprint files (max 119 characters).	string	Maximum length: 119							
file-pattern	Files matching this pattern on the server are fingerprinted. Optionally use the * and ? wildcards.	string	Maximum length: 35	*						
keep-modified	Enable so that when a file is changed on the server the FortiGate keeps the old fingerprint and adds a new fingerprint to the database.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Keep the old fingerprint and add a new fingerprint when a file is changed on the server.</td></tr><tr><td><i>disable</i></td><td>Replace the old fingerprint with the new fingerprint when a file is changed on the server.</td></tr></table>				Option	Description	<i>enable</i>	Keep the old fingerprint and add a new fingerprint when a file is changed on the server.	<i>disable</i>	Replace the old fingerprint with the new fingerprint when a file is changed on the server.
Option	Description									
<i>enable</i>	Keep the old fingerprint and add a new fingerprint when a file is changed on the server.									
<i>disable</i>	Replace the old fingerprint with the new fingerprint when a file is changed on the server.									
name	Name of the DLP fingerprint database.	string	Maximum length: 35							
password	Password required to log into the file server.	password	Not Specified							
period	Frequency for which the FortiGate checks the server for new or changed files.	option	-	none						

Parameter	Description	Type	Size	Default										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>Check the server when the FortiGate starts up.</td></tr><tr><td><i>daily</i></td><td>Check the server once a day.</td></tr><tr><td><i>weekly</i></td><td>Check the server once a week.</td></tr><tr><td><i>monthly</i></td><td>Check the server once a month.</td></tr></table>	Option	Description	<i>none</i>	Check the server when the FortiGate starts up.	<i>daily</i>	Check the server once a day.	<i>weekly</i>	Check the server once a week.	<i>monthly</i>	Check the server once a month.			
Option	Description													
<i>none</i>	Check the server when the FortiGate starts up.													
<i>daily</i>	Check the server once a day.													
<i>weekly</i>	Check the server once a week.													
<i>monthly</i>	Check the server once a month.													
remove-deleted	Enable to keep the fingerprint database up to date when a file is deleted from the server.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Keep the fingerprint database up to date when a file is deleted from the server.</td></tr><tr><td><i>disable</i></td><td>Do not check for deleted files on the server. Saves system resources.</td></tr></table>	Option	Description	<i>enable</i>	Keep the fingerprint database up to date when a file is deleted from the server.	<i>disable</i>	Do not check for deleted files on the server. Saves system resources.							
Option	Description													
<i>enable</i>	Keep the fingerprint database up to date when a file is deleted from the server.													
<i>disable</i>	Do not check for deleted files on the server. Saves system resources.													
scan-on-creation	Enable to keep the fingerprint database up to date when a file is added or changed on the server.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Keep the fingerprint database up to date when a file is added or changed on the server.</td></tr><tr><td><i>disable</i></td><td>Do not check for added or changed files on the server. Saves system resources.</td></tr></table>	Option	Description	<i>enable</i>	Keep the fingerprint database up to date when a file is added or changed on the server.	<i>disable</i>	Do not check for added or changed files on the server. Saves system resources.							
Option	Description													
<i>enable</i>	Keep the fingerprint database up to date when a file is added or changed on the server.													
<i>disable</i>	Do not check for added or changed files on the server. Saves system resources.													
scan-subdirectories	Enable/disable scanning subdirectories to find files to create fingerprints from.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Scan subdirectories.</td></tr><tr><td><i>disable</i></td><td>Do not scan subdirectories.</td></tr></table>	Option	Description	<i>enable</i>	Scan subdirectories.	<i>disable</i>	Do not scan subdirectories.							
Option	Description													
<i>enable</i>	Scan subdirectories.													
<i>disable</i>	Do not scan subdirectories.													
sensitivity	Select a sensitivity or threat level for matches with this fingerprint database. Add sensitivities using sensitivity.	string	Maximum length: 35											
server	IPv4 or IPv6 address of the server.	string	Maximum length: 35											
server-type	Protocol used to communicate with the file server. Currently only Samba (SMB) servers are supported.	option	-	samba										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>samba</i></td><td>SAMBA server.</td></tr></table>	Option	Description	<i>samba</i>	SAMBA server.									
Option	Description													
<i>samba</i>	SAMBA server.													

Parameter	Description	Type	Size	Default																
tod-hour	Hour of the day on which to scan the server.	integer	Minimum value: 0 Maximum value: 23	1																
tod-min	Minute of the hour on which to scan the server.	integer	Minimum value: 0 Maximum value: 59	0																
username	User name required to log into the file server.	string	Maximum length: 35																	
vdom	Select the VDOM that can communicate with the file server.	option	-	mgmt																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>mgmt</td><td>Communicate with the file server through the management VDOM.</td></tr><tr><td>current</td><td>Communicate with the file server through the VDOM containing this DLP fingerprint database configuration.</td></tr></table>				Option	Description	mgmt	Communicate with the file server through the management VDOM.	current	Communicate with the file server through the VDOM containing this DLP fingerprint database configuration.										
Option	Description																			
mgmt	Communicate with the file server through the management VDOM.																			
current	Communicate with the file server through the VDOM containing this DLP fingerprint database configuration.																			
weekday	Day of the week on which to scan the server.	option	-	sunday																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>sunday</td><td>Sunday</td></tr><tr><td>monday</td><td>Monday</td></tr><tr><td>tuesday</td><td>Tuesday</td></tr><tr><td>wednesday</td><td>Wednesday</td></tr><tr><td>thursday</td><td>Thursday</td></tr><tr><td>friday</td><td>Friday</td></tr><tr><td>saturday</td><td>Saturday</td></tr></table>				Option	Description	sunday	Sunday	monday	Monday	tuesday	Tuesday	wednesday	Wednesday	thursday	Thursday	friday	Friday	saturday	Saturday
Option	Description																			
sunday	Sunday																			
monday	Monday																			
tuesday	Tuesday																			
wednesday	Wednesday																			
thursday	Thursday																			
friday	Friday																			
saturday	Saturday																			

## config dlp sensitivity

Create self-explanatory DLP sensitivity levels to be used when setting sensitivity under config fp-doc-source.

```

config dlp sensitivity
    Description: Create self-explanatory DLP sensitivity levels to be used when setting
sensitivity under config fp-doc-source.
    edit <name>
    next
end

```

## config dlp sensitivity

Parameter	Description	Type	Size	Default
name	DLP Sensitivity Levels.	string	Maximum length: 35	

## config dlp sensor

Configure DLP sensors.

```
config dlp sensor
  Description: Configure DLP sensors.
  edit <name>
    set comment {var-string}
    set dlp-log [enable|disable]
    set extended-log [enable|disable]
    set feature-set [flow|proxy]
    config filter
      Description: Set up DLP filters for this sensor.
      edit <id>
        set name {string}
        set severity [info|low|...]
        set type [file|message]
        set proto {option1}, {option2}, ...
        set filter-by [credit-card|ssn|...]
        set file-size {integer}
        set company-identifier {string}
        set sensitivity <name1>, <name2>, ...
        set match-percentage {integer}
        set file-type {integer}
        set regexp {string}
        set archive [disable|enable]
        set action [allow|log-only|...]
        set expiry {user}
      next
    end
    set full-archive-proto {option1}, {option2}, ...
    set nac-quar-log [enable|disable]
    set replacemsg-group {string}
    set summary-proto {option1}, {option2}, ...
  next
end
```

## config dlp sensor

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 255	

Parameter	Description	Type	Size	Default																						
dlp-log	Enable/disable DLP logging.	option	-	enable																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable DLP logging.</td></tr><tr><td><i>disable</i></td><td>Disable DLP logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable DLP logging.	<i>disable</i>	Disable DLP logging.																			
	Option	Description																								
	<i>enable</i>	Enable DLP logging.																								
<i>disable</i>	Disable DLP logging.																									
extended-log	Enable/disable extended logging for data leak prevention.	option	-	disable																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.																			
	Option	Description																								
	<i>enable</i>	Enable setting.																								
<i>disable</i>	Disable setting.																									
feature-set	Flow/proxy feature set.	option	-	flow																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>flow</i></td><td>Flow feature set.</td></tr><tr><td><i>proxy</i></td><td>Proxy feature set.</td></tr></table>	Option	Description	<i>flow</i>	Flow feature set.	<i>proxy</i>	Proxy feature set.																			
	Option	Description																								
	<i>flow</i>	Flow feature set.																								
<i>proxy</i>	Proxy feature set.																									
full-archive-proto	Protocols to always content archive.	option	-																							
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>smtp</i></td><td>SMTP.</td></tr><tr><td><i>pop3</i></td><td>POP3.</td></tr><tr><td><i>imap</i></td><td>IMAP.</td></tr><tr><td><i>http-get</i></td><td>HTTP GET.</td></tr><tr><td><i>http-post</i></td><td>HTTP POST.</td></tr><tr><td><i>ftp</i></td><td>FTP.</td></tr><tr><td><i>nntp</i></td><td>NNTP.</td></tr><tr><td><i>mapi</i></td><td>MAPI.</td></tr><tr><td><i>ssh</i></td><td>SFTP and SCP.</td></tr><tr><td><i>cifs</i></td><td>CIFS.</td></tr></table>	Option	Description	<i>smtp</i>	SMTP.	<i>pop3</i>	POP3.	<i>imap</i>	IMAP.	<i>http-get</i>	HTTP GET.	<i>http-post</i>	HTTP POST.	<i>ftp</i>	FTP.	<i>nntp</i>	NNTP.	<i>mapi</i>	MAPI.	<i>ssh</i>	SFTP and SCP.	<i>cifs</i>	CIFS.			
	Option	Description																								
	<i>smtp</i>	SMTP.																								
	<i>pop3</i>	POP3.																								
	<i>imap</i>	IMAP.																								
	<i>http-get</i>	HTTP GET.																								
	<i>http-post</i>	HTTP POST.																								
	<i>ftp</i>	FTP.																								
	<i>nntp</i>	NNTP.																								
	<i>mapi</i>	MAPI.																								
	<i>ssh</i>	SFTP and SCP.																								
<i>cifs</i>	CIFS.																									
nac-quar-log	Enable/disable NAC quarantine logging.	option	-	disable																						

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable NAC quarantine logging.		
	<i>disable</i>	Disable NAC quarantine logging.		
name	Name of the DLP sensor.	string	Maximum length: 35	
replacemsg-group	Replacement message group used by this DLP sensor.	string	Maximum length: 35	
summary-proto	Protocols to always log summary.	option	-	
	<b>Option</b>	<b>Description</b>		
	<i>smtp</i>	SMTP.		
	<i>pop3</i>	POP3.		
	<i>imap</i>	IMAP.		
	<i>http-get</i>	HTTP GET.		
	<i>http-post</i>	HTTP POST.		
	<i>ftp</i>	FTP.		
	<i>nnntp</i>	NNTP.		
	<i>mapi</i>	MAPI.		
	<i>ssh</i>	SFTP and SCP.		
	<i>cifs</i>	CIFS.		

### config filter

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
name	Filter name.	string	Maximum length: 35	
severity	Select the severity or threat level that matches this filter.	option	-	medium



Parameter	Description	Type	Size	Default																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>info</i></td><td>Informational.</td></tr><tr><td><i>low</i></td><td>Low.</td></tr><tr><td><i>medium</i></td><td>Medium.</td></tr><tr><td><i>high</i></td><td>High.</td></tr><tr><td><i>critical</i></td><td>Critical.</td></tr></table>	Option	Description	<i>info</i>	Informational.	<i>low</i>	Low.	<i>medium</i>	Medium.	<i>high</i>	High.	<i>critical</i>	Critical.													
	Option	Description																								
	<i>info</i>	Informational.																								
	<i>low</i>	Low.																								
	<i>medium</i>	Medium.																								
	<i>high</i>	High.																								
<i>critical</i>	Critical.																									
type	Select whether to check the content of messages (an email message) or files (downloaded files or email attachments).	option	-	file																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>file</i></td><td>Check the contents of downloaded or attached files.</td></tr><tr><td><i>message</i></td><td>Check the contents of email messages, web pages, etc.</td></tr></table>	Option	Description	<i>file</i>	Check the contents of downloaded or attached files.	<i>message</i>	Check the contents of email messages, web pages, etc.																			
	Option	Description																								
	<i>file</i>	Check the contents of downloaded or attached files.																								
<i>message</i>	Check the contents of email messages, web pages, etc.																									
proto	Check messages or files over one or more of these protocols.	option	-																							
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>smtp</i></td><td>SMTP.</td></tr><tr><td><i>pop3</i></td><td>POP3.</td></tr><tr><td><i>imap</i></td><td>IMAP.</td></tr><tr><td><i>http-get</i></td><td>HTTP GET.</td></tr><tr><td><i>http-post</i></td><td>HTTP POST.</td></tr><tr><td><i>ftp</i></td><td>FTP.</td></tr><tr><td><i>nntp</i></td><td>NNTP.</td></tr><tr><td><i>mapi</i></td><td>MAPI.</td></tr><tr><td><i>ssh</i></td><td>SFTP and SCP.</td></tr><tr><td><i>cifs</i></td><td>CIFS.</td></tr></table>	Option	Description	<i>smtp</i>	SMTP.	<i>pop3</i>	POP3.	<i>imap</i>	IMAP.	<i>http-get</i>	HTTP GET.	<i>http-post</i>	HTTP POST.	<i>ftp</i>	FTP.	<i>nntp</i>	NNTP.	<i>mapi</i>	MAPI.	<i>ssh</i>	SFTP and SCP.	<i>cifs</i>	CIFS.			
	Option	Description																								
	<i>smtp</i>	SMTP.																								
	<i>pop3</i>	POP3.																								
	<i>imap</i>	IMAP.																								
	<i>http-get</i>	HTTP GET.																								
	<i>http-post</i>	HTTP POST.																								
	<i>ftp</i>	FTP.																								
	<i>nntp</i>	NNTP.																								
	<i>mapi</i>	MAPI.																								
<i>ssh</i>	SFTP and SCP.																									
<i>cifs</i>	CIFS.																									
filter-by	Select the type of content to match.	option	-	credit-card																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>credit-card</i></td><td>Match credit cards.</td></tr><tr><td><i>ssn</i></td><td>Match social security numbers.</td></tr></table>	Option	Description	<i>credit-card</i>	Match credit cards.	<i>ssn</i>	Match social security numbers.																			
	Option	Description																								
	<i>credit-card</i>	Match credit cards.																								
<i>ssn</i>	Match social security numbers.																									

Parameter	Description	Type	Size	Default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>regexp</i></td><td>Use a regular expression to match content.</td></tr><tr><td><i>file-type</i></td><td>Match a DLP file pattern list.</td></tr><tr><td><i>file-size</i></td><td>Match any file over with a size over the threshold.</td></tr><tr><td><i>fingerprint</i></td><td>Match against a fingerprint sensitivity.</td></tr><tr><td><i>watermark</i></td><td>Look for defined file watermarks.</td></tr><tr><td><i>encrypted</i></td><td>Look for encrypted files.</td></tr></table>	Option	Description	<i>regexp</i>	Use a regular expression to match content.	<i>file-type</i>	Match a DLP file pattern list.	<i>file-size</i>	Match any file over with a size over the threshold.	<i>fingerprint</i>	Match against a fingerprint sensitivity.	<i>watermark</i>	Look for defined file watermarks.	<i>encrypted</i>	Look for encrypted files.			
	Option	Description																
	<i>regexp</i>	Use a regular expression to match content.																
	<i>file-type</i>	Match a DLP file pattern list.																
	<i>file-size</i>	Match any file over with a size over the threshold.																
	<i>fingerprint</i>	Match against a fingerprint sensitivity.																
	<i>watermark</i>	Look for defined file watermarks.																
<i>encrypted</i>	Look for encrypted files.																	
file-size	Match files this size or larger.	integer	Minimum value: 0 Maximum value: 4294967295	10 **														
company-identifier	Enter a company identifier watermark to match. Only watermarks that your company has placed on the files are matched.	string	Maximum length: 35															
sensitivity <name>	Select a DLP file pattern sensitivity to match. Select a DLP sensitivity.	string	Maximum length: 35															
match-percentage *	Percentage of fingerprints in the fingerprint databases designated with the selected sensitivity to match.	integer	Minimum value: 1 Maximum value: 100	10														
file-type	Select the number of a DLP file pattern table to match.	integer	Minimum value: 0 Maximum value: 4294967295	0														
regexp	Enter a regular expression to match (max. 255 characters).	string	Maximum length: 255															
archive	Enable/disable DLP archiving.	option	-	disable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>No DLP archiving.</td></tr><tr><td><i>enable</i></td><td>Enable full DLP archiving.</td></tr></table>	Option	Description	<i>disable</i>	No DLP archiving.	<i>enable</i>	Enable full DLP archiving.											
	Option	Description																
	<i>disable</i>	No DLP archiving.																
<i>enable</i>	Enable full DLP archiving.																	
action	Action to take with content that this DLP sensor matches.	option	-	allow														

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow the content to pass through the FortiGate and do not create a log message.		
	<i>log-only</i>	Allow the content to pass through the FortiGate, but write a log message.		
	<i>block</i>	Block the content and write a log message.		
	<i>quarantine-ip</i>	Quarantine all traffic from the IP address and write a log message.		
expiry	Quarantine duration in days, hours, minutes (format = dddhhmm).		user	Not Specified 5m

\* This parameter may not exist in some models.

\*\* Values may differ between models.

## config dlp settings



This command is available for model(s): FortiGate 1000D, FortiGate 101E, FortiGate 101F, FortiGate 1101E, FortiGate 1200D, FortiGate 1500DT, FortiGate 1500D, FortiGate 1801F, FortiGate 2000E, FortiGate 201E, FortiGate 201F, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3001F, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3301E, FortiGate 3401E, FortiGate 3501F, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4201F, FortiGate 4401F, FortiGate 5001E1, FortiGate 501E, FortiGate 601E, FortiGate 601F, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80F Bypass, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 91E, FortiGate VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 1100E, FortiGate 140E-POE, FortiGate 140E, FortiGate 1800F, FortiGate 200E, FortiGate 200F, FortiGate 2200E, FortiGate 3000F, FortiGate 300E, FortiGate 3300E, FortiGate 3400E, FortiGate 3500F, FortiGate 3600E, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 4200F, FortiGate 4400F, FortiGate 5001E, FortiGate 500E, FortiGate 600E, FortiGate 600F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F-POE, FortiGate 80F, FortiGate 90E, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E.

Designate logical storage for DLP fingerprint database.

```
config dlp settings
```

```
Description: Designate logical storage for DLP fingerprint database.
```

```
set cache-mem-percent {integer}
```

```
set chunk-size {integer}
```

```
set db-mode [stop-adding|remove-modified-then-oldest|...]
```

```

    set size {integer}
    set storage-device {string}
end

```

## config dlp settings

Parameter	Description	Type	Size	Default
cache-mem-percent	Maximum percentage of available memory allocated to caching.	integer	Minimum value: 1 Maximum value: 15	2
chunk-size	Maximum fingerprint chunk size. Caution, changing this setting will flush the entire database.	integer	Minimum value: 100 Maximum value: 100000	2800
db-mode	Behavior when the maximum size is reached.	option	-	stop-adding
	Option	Description		
	stop-adding	Stop adding entries.		
	remove-modified-then-oldest	Remove modified chunks first, then oldest file entries.		
	remove-oldest	Remove the oldest files first.		
size	Maximum total size of files within the storage (MB).	integer	Minimum value: 16 Maximum value: 4294967295	16
storage-device	Storage device name.	string	Maximum length: 35	

## dnsfilter

This section includes syntax for the following commands:

- [config dnsfilter domain-filter on page 105](#)
- [config dnsfilter profile on page 106](#)

### config dnsfilter domain-filter

Configure DNS domain filters.

```
config dnsfilter domain-filter
  Description: Configure DNS domain filters.
  edit <id>
    set comment {var-string}
    config entries
      Description: DNS domain filter entries.
      edit <id>
        set domain {string}
        set type [simple|regex|...]
        set action [block|allow|...]
        set status [enable|disable]
      next
    end
    set name {string}
  next
end
```

### config dnsfilter domain-filter

Parameter	Description	Type	Size	Default
comment	Optional comments.	var-string	Maximum length: 255	
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
name	Name of table.	string	Maximum length: 63	

## config entries

Parameter	Description	Type	Size	Default								
id	Id.	integer	Minimum value: 0 Maximum value: 4294967295	0								
domain	Domain entries to be filtered.	string	Maximum length: 511									
type	DNS domain filter type.	option	-	simple								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>simple</i></td><td>Simple domain string.</td></tr><tr><td><i>regex</i></td><td>Regular expression domain string.</td></tr><tr><td><i>wildcard</i></td><td>Wildcard domain string.</td></tr></table>				Option	Description	<i>simple</i>	Simple domain string.	<i>regex</i>	Regular expression domain string.	<i>wildcard</i>	Wildcard domain string.
	Option	Description										
	<i>simple</i>	Simple domain string.										
	<i>regex</i>	Regular expression domain string.										
<i>wildcard</i>	Wildcard domain string.											
action	Action to take for domain filter matches.	option	-	block								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>block</i></td><td>Block DNS requests matching the domain filter.</td></tr><tr><td><i>allow</i></td><td>Allow DNS requests matching the domain filter without logging.</td></tr><tr><td><i>monitor</i></td><td>Allow DNS requests matching the domain filter with logging.</td></tr></table>				Option	Description	<i>block</i>	Block DNS requests matching the domain filter.	<i>allow</i>	Allow DNS requests matching the domain filter without logging.	<i>monitor</i>	Allow DNS requests matching the domain filter with logging.
	Option	Description										
	<i>block</i>	Block DNS requests matching the domain filter.										
	<i>allow</i>	Allow DNS requests matching the domain filter without logging.										
<i>monitor</i>	Allow DNS requests matching the domain filter with logging.											
status	Enable/disable this domain filter.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable this domain filter.</td></tr><tr><td><i>disable</i></td><td>Disable this domain filter.</td></tr></table>				Option	Description	<i>enable</i>	Enable this domain filter.	<i>disable</i>	Disable this domain filter.		
	Option	Description										
	<i>enable</i>	Enable this domain filter.										
<i>disable</i>	Disable this domain filter.											

## config dnsfilter profile

Configure DNS domain filter profile.

```
config dnsfilter profile
  Description: Configure DNS domain filter profile.
  edit <name>
    set block-action [block|redirect|...]
    set block-botnet [disable|enable]
    set comment {var-string}
    config dns-translation
      Description: DNS translation settings.
      edit <id>
        set addr-type [ipv4|ipv6]
```

```

        set src {ipv4-address}
        set dst {ipv4-address}
        set netmask {ipv4-netmask}
        set status [enable|disable]
        set src6 {ipv6-address}
        set dst6 {ipv6-address}
        set prefix {integer}
    next
end
config domain-filter
    Description: Domain filter settings.
    set domain-filter-table {integer}
end
set external-ip-blocklist <name1>, <name2>, ...
config ftgd-dns
    Description: FortiGuard DNS Filter settings.
    set options {option1}, {option2}, ...
    config filters
        Description: FortiGuard DNS domain filters.
        edit <id>
            set category {integer}
            set action [block|monitor]
            set log [enable|disable]
        next
    end
end
set log-all-domain [enable|disable]
set redirect-portal {ipv4-address}
set redirect-portal6 {ipv6-address}
set safe-search [disable|enable]
set sdns-domain-log [enable|disable]
set sdns-ftgd-err-log [enable|disable]
set youtube-restrict [strict|moderate]
next
end

```

## config dnsfilter profile

Parameter	Description	Type	Size	Default								
block-action	Action to take for blocked domains.	option	-	redirect								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>block</i></td><td>Return NXDOMAIN for blocked domains.</td></tr><tr><td><i>redirect</i></td><td>Redirect blocked domains to SDNS portal.</td></tr><tr><td><i>block-sevrfail</i></td><td>Return SERVFAIL for blocked domains.</td></tr></table>				Option	Description	<i>block</i>	Return NXDOMAIN for blocked domains.	<i>redirect</i>	Redirect blocked domains to SDNS portal.	<i>block-sevrfail</i>	Return SERVFAIL for blocked domains.
	Option	Description										
	<i>block</i>	Return NXDOMAIN for blocked domains.										
	<i>redirect</i>	Redirect blocked domains to SDNS portal.										
<i>block-sevrfail</i>	Return SERVFAIL for blocked domains.											
block-botnet	Enable/disable blocking botnet C&C DNS lookups.	option	-	disable								

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable blocking botnet C&C DNS lookups.		
	<i>enable</i>	Enable blocking botnet C&C DNS lookups.		
comment	Comment.	var-string	Maximum length: 255	
external-ip-blocklist <name>	One or more external IP block lists. External domain block list name.	string	Maximum length: 79	
log-all-domain	Enable/disable logging of all domains visited (detailed DNS logging).	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable logging of all domains visited.		
	<i>disable</i>	Disable logging of all domains visited.		
name	Profile name.	string	Maximum length: 35	
redirect-portal	IPv4 address of the SDNS redirect portal.	ipv4-address	Not Specified	0.0.0.0
redirect-portal6	IPv6 address of the SDNS redirect portal.	ipv6-address	Not Specified	::
safe-search	Enable/disable Google, Bing, YouTube, Qwant, DuckDuckGo safe search.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable Google, Bing, YouTube, Qwant, DuckDuckGo safe search.		
	<i>enable</i>	Enable Google, Bing, YouTube, Qwant, DuckDuckGo safe search.		
sdns-domain-log	Enable/disable domain filtering and botnet domain logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable domain filtering and botnet domain logging.		
	<i>disable</i>	Disable domain filtering and botnet domain logging.		
sdns-ftgd-err-log	Enable/disable FortiGuard SDNS rating error logging.	option	-	enable



Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable FortiGuard SDNS rating error logging.		
	<i>disable</i>	Disable FortiGuard SDNS rating error logging.		
youtube-restrict	Set safe search for YouTube restriction level.	option	-	strict
	<b>Option</b>	<b>Description</b>		
	<i>strict</i>	Enable strict safe search for YouTube.		
	<i>moderate</i>	Enable moderate safe search for YouTube.		

### config dns-translation

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
addr-type	DNS translation type (IPv4 or IPv6).	option	-	ipv4
	<b>Option</b>	<b>Description</b>		
	<i>ipv4</i>	IPv4 address type.		
	<i>ipv6</i>	IPv6 address type.		
src	IPv4 address or subnet on the internal network to compare with the resolved address in DNS query replies. If the resolved address matches, the resolved address is substituted with dst.	ipv4-address	Not Specified	0.0.0.0
dst	IPv4 address or subnet on the external network to substitute for the resolved address in DNS query replies. Can be single IP address or subnet on the external network, but number of addresses must equal number of mapped IP addresses in src.	ipv4-address	Not Specified	0.0.0.0
netmask	If src and dst are subnets rather than single IP addresses, enter the netmask for both src and dst.	ipv4-netmask	Not Specified	255.255.255.255
status	Enable/disable this DNS translation entry.	option	-	enable

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable this DNS translation.		
	<i>disable</i>	Disable this DNS translation.		
src6	IPv6 address or subnet on the internal network to compare with the resolved address in DNS query replies. If the resolved address matches, the resolved address is substituted with dst6.	ipv6-address	Not Specified	::
dst6	IPv6 address or subnet on the external network to substitute for the resolved address in DNS query replies. Can be single IP address or subnet on the external network, but number of addresses must equal number of mapped IP addresses in src6.	ipv6-address	Not Specified	::
prefix	If src6 and dst6 are subnets rather than single IP addresses, enter the prefix for both src6 and dst6.	integer	Minimum value: 1 Maximum value: 128	128

### config domain-filter

Parameter	Description	Type	Size	Default
domain-filter-table	DNS domain filter table ID.	integer	Minimum value: 0 Maximum value: 4294967295	0

### config ftgd-dns

Parameter	Description	Type	Size	Default
options	FortiGuard DNS filter options.	option	-	
	Option	Description		
	<i>error-allow</i>	Allow all domains when FortiGuard DNS servers fail.		
	<i>ftgd-disable</i>	Disable FortiGuard DNS domain rating.		

## config filters

Parameter	Description	Type	Size	Default						
id	ID number.	integer	Minimum value: 0 Maximum value: 255	0						
category	Category number.	integer	Minimum value: 0 Maximum value: 255	0						
action	Action to take for DNS requests matching the category.	option	-	monitor						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>block</i></td><td>Block DNS requests matching the category.</td></tr><tr><td><i>monitor</i></td><td>Allow DNS requests matching the category and log the result.</td></tr></table>	Option	Description	<i>block</i>	Block DNS requests matching the category.	<i>monitor</i>	Allow DNS requests matching the category and log the result.			
Option	Description									
<i>block</i>	Block DNS requests matching the category.									
<i>monitor</i>	Allow DNS requests matching the category and log the result.									
log	Enable/disable DNS filter logging for this DNS profile.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable DNS filter logging.</td></tr><tr><td><i>disable</i></td><td>Disable DNS filter logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable DNS filter logging.	<i>disable</i>	Disable DNS filter logging.			
Option	Description									
<i>enable</i>	Enable DNS filter logging.									
<i>disable</i>	Disable DNS filter logging.									

## dpdk

This section includes syntax for the following commands:

- [config dpdk cpus on page 112](#)
- [config dpdk global on page 113](#)

### config dpdk cpus



This command is available for model(s): FortiGate VM64.

It is not available for: FortiGate 1000D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

Configure CPUs enabled to run engines in each DPDK stage.

```
config dpdk cpus
    Description: Configure CPUs enabled to run engines in each DPDK stage.
    set rx-cpus {string}
    set vnp-cpus {string}
    set ips-cpus {string}
    set tx-cpus {string}
    set isolated-cpus {string}
end
```

## config dpdk cpus

Parameter	Description	Type	Size	Default
rx-cpus	CPUs enabled to run DPDK RX engines.	string	Maximum length: 1022	all
vnp-cpus	CPUs enabled to run DPDK VNP engines.	string	Maximum length: 1022	all
ips-cpus	CPUs enabled to run DPDK IPS engines.	string	Maximum length: 1022	all
tx-cpus	CPUs enabled to run DPDK TX engines.	string	Maximum length: 1022	all
isolated-cpus	CPUs isolated to run only the DPDK engines with the exception of processes that have affinity explicitly set by either a user configuration or by their implementation.	string	Maximum length: 1022	none

## config dpdk global



This command is available for model(s): FortiGate VM64.

It is not available for: FortiGate 1000D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

Configure global DPDK options.

```
config dpdk global
    Description: Configure global DPDK options.
    set status [disable|enable]
```

```

set interface <interface-name1>, <interface-name2>, ...
set multiqueue [disable|enable]
set sleep-on-idle [disable|enable]
set elasticbuffer [disable|enable]
set per-session-accounting [disable|traffic-log-only|...]
set ipsec-offload [disable|enable]
set hugepage-percentage {integer}
set mbufpool-percentage {integer}
end

```

## config dpdk global

Parameter	Description	Type	Size	Default
status	Enable/disable DPDK operation for the entire system.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable DPDK operation.		
	<i>enable</i>	Enable DPDK operation. *The minimum system requirements for DPDK is 2 vCPUs and 4GB memory.		
interface <interface-name>	Physical interfaces that enable DPDK. Physical interface name.	string	Maximum length: 31	
multiqueue	Enable/disable multi-queue RX/TX support for all DPDK ports.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable multi-queue RX/TX support for DPDK ports.		
	<i>enable</i>	Enable multi-queue RX/TX support for DPDK ports.		
sleep-on-idle	Enable/disable sleep-on-idle support for all FDH engines.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable sleep-on-idle support for FDH engines.		
	<i>enable</i>	Enable sleep-on-idle support for FDH engines.		
elasticbuffer	Enable/disable elasticbuffer support for all DPDK ports.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable elasticbuffer support for DPDK ports.		
	<i>enable</i>	Enable elasticbuffer support for DPDK ports.		

Parameter	Description	Type	Size	Default
per-session-accounting	Enable/disable per-session accounting.	option	-	traffic-log-only
	Option	Description		
	disable	Disable per-session accounting.		
	traffic-log-only	Enable per-session accounting only for VNP sessions with traffic logging turned on in firewall policy.		
	enable	Enable per-session accounting for all VNP sessions. *Affect performance.		
ipsec-offload	Enable/disable DPDK IPsec phase 2 offloading.	option	-	disable
	Option	Description		
	disable	Disable DPDK IPsec phase 2 offloading.		
	enable	Enable DPDK IPsec phase 2 offloading.		
hugepage-percentage	Percentage of main memory allocated to hugepages, which are available for DPDK operation.	integer	Minimum value: 15 Maximum value: 50	30
mbufpool-percentage	Percentage of main memory allocated to DPDK packet buffer.	integer	Minimum value: 10 Maximum value: 45	25

## emailfilter

This section includes syntax for the following commands:

- [config emailfilter block-allow-list on page 116](#)
- [config emailfilter bword on page 118](#)
- [config emailfilter dnsbl on page 120](#)
- [config emailfilter fortishield on page 121](#)
- [config emailfilter iptrust on page 122](#)
- [config emailfilter mheader on page 123](#)
- [config emailfilter options on page 125](#)
- [config emailfilter profile on page 125](#)

### config emailfilter block-allow-list

Configure anti-spam block/allow list.

```
config emailfilter block-allow-list
  Description: Configure anti-spam block/allow list.
  edit <id>
    set comment {var-string}
    config entries
      Description: Anti-spam block/allow entries.
      edit <id>
        set status [enable|disable]
        set type [ip|email]
        set action [reject|spam|...]
        set addr-type [ipv4|ipv6]
        set ip4-subnet {ipv4-classnet}
        set ip6-subnet {ipv6-network}
        set pattern-type [wildcard|regexp]
        set email-pattern {string}
      next
    end
    set name {string}
  next
end
```

### config emailfilter block-allow-list

Parameter	Description	Type	Size	Default
comment	Optional comments.	var-string	Maximum length: 255	



Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
name	Name of table.	string	Maximum length: 63	

### config entries

Parameter	Description	Type	Size	Default								
status	Enable/disable status.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable status.</td></tr><tr><td><i>disable</i></td><td>Disable status.</td></tr></table>				Option	Description	<i>enable</i>	Enable status.	<i>disable</i>	Disable status.		
	Option	Description										
	<i>enable</i>	Enable status.										
<i>disable</i>	Disable status.											
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0								
type	Entry type.	option	-	ip								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ip</i></td><td>By IP address.</td></tr><tr><td><i>email</i></td><td>By email address.</td></tr></table>				Option	Description	<i>ip</i>	By IP address.	<i>email</i>	By email address.		
	Option	Description										
	<i>ip</i>	By IP address.										
<i>email</i>	By email address.											
action	Reject, mark as spam or good email.	option	-	spam								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>reject</i></td><td>Reject the connection.</td></tr><tr><td><i>spam</i></td><td>Mark as spam email.</td></tr><tr><td><i>clear</i></td><td>Mark as good email.</td></tr></table>				Option	Description	<i>reject</i>	Reject the connection.	<i>spam</i>	Mark as spam email.	<i>clear</i>	Mark as good email.
	Option	Description										
	<i>reject</i>	Reject the connection.										
	<i>spam</i>	Mark as spam email.										
<i>clear</i>	Mark as good email.											
addr-type	IP address type.	option	-	ipv4								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ipv4</i></td><td>IPv4 Address type.</td></tr><tr><td><i>ipv6</i></td><td>IPv6 Address type.</td></tr></table>				Option	Description	<i>ipv4</i>	IPv4 Address type.	<i>ipv6</i>	IPv6 Address type.		
	Option	Description										
	<i>ipv4</i>	IPv4 Address type.										
<i>ipv6</i>	IPv6 Address type.											

Parameter	Description	Type	Size	Default
ip4-subnet	IPv4 network address/subnet mask bits.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0
ip6-subnet	IPv6 network address/subnet mask bits.	ipv6-network	Not Specified	::/128
pattern-type	Wildcard pattern or regular expression.	option	-	wildcard
	Option	Description		
	wildcard	Wildcard pattern.		
	regexp	Perl regular expression.		
email-pattern	Email address pattern.	string	Maximum length: 127	

## config emailfilter bword

Configure AntiSpam banned word list.

```

config emailfilter bword
    Description: Configure AntiSpam banned word list.
    edit <id>
        set comment {var-string}
        config entries
            Description: Spam filter banned word.
            edit <id>
                set status [enable|disable]
                set pattern {string}
                set pattern-type [wildcard|regexp]
                set action [spam|clear]
                set where [subject|body|...]
                set language [western|simch|...]
                set score {integer}
            next
        end
        set name {string}
    next
end

```

## config emailfilter bword

Parameter	Description	Type	Size	Default
comment	Optional comments.	var-string	Maximum length: 255	

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
name	Name of table.	string	Maximum length: 63	

### config entries

Parameter	Description	Type	Size	Default						
status	Enable/disable status.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable status.</td></tr><tr><td><i>disable</i></td><td>Disable status.</td></tr></table>				Option	Description	<i>enable</i>	Enable status.	<i>disable</i>	Disable status.
	Option	Description								
	<i>enable</i>	Enable status.								
<i>disable</i>	Disable status.									
id	Banned word entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0						
pattern	Pattern for the banned word.	string	Maximum length: 127							
pattern-type	Wildcard pattern or regular expression.	option	-	wildcard						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>wildcard</i></td><td>Wildcard pattern.</td></tr><tr><td><i>regex</i></td><td>Perl regular expression.</td></tr></table>				Option	Description	<i>wildcard</i>	Wildcard pattern.	<i>regex</i>	Perl regular expression.
	Option	Description								
	<i>wildcard</i>	Wildcard pattern.								
<i>regex</i>	Perl regular expression.									
action	Mark spam or good.	option	-	spam						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>spam</i></td><td>Mark as spam email.</td></tr><tr><td><i>clear</i></td><td>Mark as good email.</td></tr></table>				Option	Description	<i>spam</i>	Mark as spam email.	<i>clear</i>	Mark as good email.
	Option	Description								
	<i>spam</i>	Mark as spam email.								
<i>clear</i>	Mark as good email.									
where	Component of the email to be scanned.	option	-	all						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>subject</i></td><td>Banned word in email subject.</td></tr></table>				Option	Description	<i>subject</i>	Banned word in email subject.		
	Option	Description								
<i>subject</i>	Banned word in email subject.									

Parameter	Description	Type	Size	Default																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>body</i></td><td>Banned word in email body.</td></tr><tr><td><i>all</i></td><td>Banned word in both subject and body.</td></tr></table>	Option	Description	<i>body</i>	Banned word in email body.	<i>all</i>	Banned word in both subject and body.															
	Option	Description																				
	<i>body</i>	Banned word in email body.																				
<i>all</i>	Banned word in both subject and body.																					
language	Language for the banned word.	option	-	western																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>western</i></td><td>Western.</td></tr><tr><td><i>simch</i></td><td>Simplified Chinese.</td></tr><tr><td><i>trach</i></td><td>Traditional Chinese.</td></tr><tr><td><i>japanese</i></td><td>Japanese.</td></tr><tr><td><i>korean</i></td><td>Korean.</td></tr><tr><td><i>french</i></td><td>French.</td></tr><tr><td><i>thai</i></td><td>Thai.</td></tr><tr><td><i>spanish</i></td><td>Spanish.</td></tr></table>	Option	Description	<i>western</i>	Western.	<i>simch</i>	Simplified Chinese.	<i>trach</i>	Traditional Chinese.	<i>japanese</i>	Japanese.	<i>korean</i>	Korean.	<i>french</i>	French.	<i>thai</i>	Thai.	<i>spanish</i>	Spanish.			
	Option	Description																				
	<i>western</i>	Western.																				
	<i>simch</i>	Simplified Chinese.																				
	<i>trach</i>	Traditional Chinese.																				
	<i>japanese</i>	Japanese.																				
	<i>korean</i>	Korean.																				
	<i>french</i>	French.																				
	<i>thai</i>	Thai.																				
<i>spanish</i>	Spanish.																					
score	Score value.	integer	Minimum value: 1 Maximum value: 99999	10																		

## config emailfilter dnsbl

Configure AntiSpam DNSBL/ORBL.

```

config emailfilter dnsbl
    Description: Configure AntiSpam DNSBL/ORBL.
    edit <id>
        set comment {var-string}
        config entries
            Description: Spam filter DNSBL and ORBL server.
            edit <id>
                set status [enable|disable]
                set server {string}
                set action [reject|spam]
            next
        next
    end
    set name {string}
next
end

```

## config emailfilter dnsbl

Parameter	Description	Type	Size	Default
comment	Optional comments.	var-string	Maximum length: 255	
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
name	Name of table.	string	Maximum length: 63	

## config entries

Parameter	Description	Type	Size	Default
status	Enable/disable status.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable status.		
	<i>disable</i>	Disable status.		
id	DNSBL/ORBL entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
server	DNSBL or ORBL server name.	string	Maximum length: 127	
action	Reject connection or mark as spam email.	option	-	spam
	<b>Option</b>	<b>Description</b>		
	<i>reject</i>	Reject the connection.		
	<i>spam</i>	Mark as spam email.		

## config emailfilter fortishield

Configure FortiGuard - AntiSpam.

```
config emailfilter fortishield
  Description: Configure FortiGuard - AntiSpam.
  set spam-submit-force [enable|disable]
  set spam-submit-srv {string}
```

```

    set spam-submit-txt2htm [enable|disable]
end

```

## config emailfilter fortishield

Parameter	Description	Type	Size	Default
spam-submit-force	Enable/disable force insertion of a new mime entity for the submission text.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
spam-submit-srv	Hostname of the spam submission server.	string	Maximum length: 63	www.nospammer.net
spam-submit-txt2htm	Enable/disable conversion of text email to HTML email.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

## config emailfilter iptrust

Configure AntiSpam IP trust.

```

config emailfilter iptrust
    Description: Configure AntiSpam IP trust.
    edit <id>
        set comment {var-string}
        config entries
            Description: Spam filter trusted IP addresses.
            edit <id>
                set status [enable|disable]
                set addr-type [ipv4|ipv6]
                set ip4-subnet {ipv4-classnet}
                set ip6-subnet {ipv6-network}
            next
        end
        set name {string}
    next
end

```

## config emailfilter iptrust

Parameter	Description	Type	Size	Default
comment	Optional comments.	var-string	Maximum length: 255	
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
name	Name of table.	string	Maximum length: 63	

## config entries

Parameter	Description	Type	Size	Default						
status	Enable/disable status.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable status.</td></tr><tr><td><i>disable</i></td><td>Disable status.</td></tr></table>				Option	Description	<i>enable</i>	Enable status.	<i>disable</i>	Disable status.
	Option	Description								
	<i>enable</i>	Enable status.								
<i>disable</i>	Disable status.									
id	Trusted IP entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0						
addr-type	Type of address.	option	-	ipv4						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ipv4</i></td><td>IPv4 Address type.</td></tr><tr><td><i>ipv6</i></td><td>IPv6 Address type.</td></tr></table>				Option	Description	<i>ipv4</i>	IPv4 Address type.	<i>ipv6</i>	IPv6 Address type.
	Option	Description								
	<i>ipv4</i>	IPv4 Address type.								
<i>ipv6</i>	IPv6 Address type.									
ip4-subnet	IPv4 network address or network address/subnet mask bits.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0						
ip6-subnet	IPv6 network address/subnet mask bits.	ipv6-network	Not Specified	::/128						

## config emailfilter mheader

Configure AntiSpam MIME header.

```

config emailfilter mheader
  Description: Configure AntiSpam MIME header.
  edit <id>
    set comment {var-string}
    config entries
      Description: Spam filter mime header content.
      edit <id>
        set status [enable|disable]
        set fieldname {string}
        set fieldbody {string}
        set pattern-type [wildcard|regexp]
        set action [spam|clear]
      next
    end
  set name {string}
next
end

```

### config emailfilter mheader

Parameter	Description	Type	Size	Default
comment	Optional comments.	var-string	Maximum length: 255	
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
name	Name of table.	string	Maximum length: 63	

### config entries

Parameter	Description	Type	Size	Default						
status	Enable/disable status.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable status.</td></tr><tr><td><i>disable</i></td><td>Disable status.</td></tr></table>				Option	Description	<i>enable</i>	Enable status.	<i>disable</i>	Disable status.
	Option	Description								
	<i>enable</i>	Enable status.								
	<i>disable</i>	Disable status.								
id	Mime header entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0						



Parameter	Description	Type	Size	Default						
fieldname	Pattern for header field name.	string	Maximum length: 63							
fieldbody	Pattern for the header field body.	string	Maximum length: 127							
pattern-type	Wildcard pattern or regular expression.	option	-	wildcard						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>wildcard</td><td>Wildcard pattern.</td></tr><tr><td>regex</td><td>Perl regular expression.</td></tr></table>				Option	Description	wildcard	Wildcard pattern.	regex	Perl regular expression.
Option	Description									
wildcard	Wildcard pattern.									
regex	Perl regular expression.									
action	Mark spam or good.	option	-	spam						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>spam</td><td>Mark as spam email.</td></tr><tr><td>clear</td><td>Mark as good email.</td></tr></table>				Option	Description	spam	Mark as spam email.	clear	Mark as good email.
Option	Description									
spam	Mark as spam email.									
clear	Mark as good email.									

## config emailfilter options

Configure AntiSpam options.

```
config emailfilter options
    Description: Configure AntiSpam options.
    set dns-timeout {integer}
end
```

## config emailfilter options

Parameter	Description	Type	Size	Default
dns-timeout	DNS query time out.	integer	Minimum value: 1 Maximum value: 30	7

## config emailfilter profile

Configure Email Filter profiles.

```
config emailfilter profile
    Description: Configure Email Filter profiles.
    edit <name>
        set comment {var-string}
        set external [enable|disable]
```

```

set feature-set [flow|proxy]
config gmail
    Description: Gmail.
    set log-all [disable|enable]
end
config imap
    Description: IMAP.
    set log-all [disable|enable]
    set action [pass|tag]
    set tag-type {option1}, {option2}, ...
    set tag-msg {string}
end
config mapi
    Description: MAPI.
    set log-all [disable|enable]
    set action [pass|discard]
end
config msn-hotmail
    Description: MSN Hotmail.
    set log-all [disable|enable]
end
set options {option1}, {option2}, ...
config other-webmails
    Description: Other supported webmails.
    set log-all [disable|enable]
end
config pop3
    Description: POP3.
    set log-all [disable|enable]
    set action [pass|tag]
    set tag-type {option1}, {option2}, ...
    set tag-msg {string}
end
set replacemsg-group {string}
config smtp
    Description: SMTP.
    set log-all [disable|enable]
    set action [pass|tag|...]
    set tag-type {option1}, {option2}, ...
    set tag-msg {string}
    set hdrp [disable|enable]
    set local-override [disable|enable]
end
set spam-bal-table {integer}
set spam-bword-table {integer}
set spam-bword-threshold {integer}
set spam-filtering [enable|disable]
set spam-iptrust-table {integer}
set spam-log [disable|enable]
set spam-log-fortiguard-response [disable|enable]
set spam-mheader-table {integer}
set spam-rbl-table {integer}
config yahoo-mail
    Description: Yahoo! Mail.
    set log-all [disable|enable]
end

```

next  
end

## config emailfilter profile

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 255	
external	Enable/disable external Email inspection.	option	-	disable
	Option	Description		
	enable	Enable setting.		
	disable	Disable setting.		
feature-set	Flow/proxy feature set.	option	-	flow
	Option	Description		
	flow	Flow feature set.		
	proxy	Proxy feature set.		
name	Profile name.	string	Maximum length: 35	
options	Options.	option	-	
	Option	Description		
	bannedword	Content block.		
	spambal	Block/allow list.		
	spamfsip	Email IP address FortiGuard AntiSpam block list check.		
	spamfssubmit	Add FortiGuard AntiSpam spam submission text.		
	spamfschksum	Email checksum FortiGuard AntiSpam check.		
	spamfsurl	Email content URL FortiGuard AntiSpam check.		
	spamhelodns	Email helo/ehlo domain DNS check.		
	spamraddrdns	Email return address DNS check.		
	spamrbl	Email DNSBL & ORBL check.		
	spamhdrcheck	Email mime header check.		
	spamfshish	Email content phishing URL FortiGuard AntiSpam check.		
replacemsg-group	Replacement message group.	string	Maximum length: 35	

Parameter	Description	Type	Size	Default
spam-bal-table	Anti-spam block/allow list table ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
spam-bword-table	Anti-spam banned word table ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
spam-bword-threshold	Spam banned word threshold.	integer	Minimum value: 0 Maximum value: 2147483647	10
spam-filtering	Enable/disable spam filtering.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
spam-iptrust-table	Anti-spam IP trust table ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
spam-log	Enable/disable spam logging for email filtering.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable spam logging for email filtering.		
	<i>enable</i>	Enable spam logging for email filtering.		
spam-log-fortiguard-response	Enable/disable logging FortiGuard spam response.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable logging FortiGuard spam response.		
	<i>enable</i>	Enable logging FortiGuard spam response.		

Parameter	Description	Type	Size	Default
spam-mheader-table	Anti-spam MIME header table ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
spam-rbl-table	Anti-spam DNSBL table ID.	integer	Minimum value: 0 Maximum value: 4294967295	0

### config gmail

Parameter	Description	Type	Size	Default
log-all	Enable/disable logging of all email traffic.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable logging of all email traffic.		
	<i>enable</i>	Enable logging of all email traffic.		

### config imap

Parameter	Description	Type	Size	Default						
log-all	Enable/disable logging of all email traffic.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable logging of all email traffic.</td></tr><tr><td><i>enable</i></td><td>Enable logging of all email traffic.</td></tr></table>	Option	Description	<i>disable</i>	Disable logging of all email traffic.	<i>enable</i>	Enable logging of all email traffic.			
Option	Description									
<i>disable</i>	Disable logging of all email traffic.									
<i>enable</i>	Enable logging of all email traffic.									
action	Action for spam email.	option	-	tag						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>pass</i></td><td>Allow spam email to pass through.</td></tr><tr><td><i>tag</i></td><td>Tag spam email with configured text in subject or header.</td></tr></table>	Option	Description	<i>pass</i>	Allow spam email to pass through.	<i>tag</i>	Tag spam email with configured text in subject or header.			
Option	Description									
<i>pass</i>	Allow spam email to pass through.									
<i>tag</i>	Tag spam email with configured text in subject or header.									
tag-type	Tag subject or header for spam email.	option	-	subject spaminfo						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>subject</i></td><td>Prepend text to spam email subject.</td></tr></table>	Option	Description	<i>subject</i>	Prepend text to spam email subject.					
Option	Description									
<i>subject</i>	Prepend text to spam email subject.									

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>header</i>	Append a user defined mime header to spam email.		
	<i>spaminfo</i>	Append spam info to spam email header.		
tag-msg	Subject text or header added to spam email.	string	Maximum length: 63	Spam

### config mapi

Parameter	Description	Type	Size	Default
log-all	Enable/disable logging of all email traffic.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable logging of all email traffic.		
	<i>enable</i>	Enable logging of all email traffic.		
action	Action for spam email.	option	-	pass
	<b>Option</b>	<b>Description</b>		
	<i>pass</i>	Allow spam email to pass through.		
	<i>discard</i>	Discard (block) spam email.		

### config msn-hotmail

Parameter	Description	Type	Size	Default
log-all	Enable/disable logging of all email traffic.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable logging of all email traffic.		
	<i>enable</i>	Enable logging of all email traffic.		

### config other-webmails

Parameter	Description	Type	Size	Default
log-all	Enable/disable logging of all email traffic.	option	-	disable

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable logging of all email traffic.		
	<i>enable</i>	Enable logging of all email traffic.		

### config pop3

Parameter	Description	Type	Size	Default
log-all	Enable/disable logging of all email traffic.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable logging of all email traffic.		
	<i>enable</i>	Enable logging of all email traffic.		
action	Action for spam email.	option	-	tag
	<b>Option</b>	<b>Description</b>		
	<i>pass</i>	Allow spam email to pass through.		
	<i>tag</i>	Tag spam email with configured text in subject or header.		
tag-type	Tag subject or header for spam email.	option	-	subject spaminfo
	<b>Option</b>	<b>Description</b>		
	<i>subject</i>	Prepend text to spam email subject.		
	<i>header</i>	Append a user defined mime header to spam email.		
	<i>spaminfo</i>	Append spam info to spam email header.		
tag-msg	Subject text or header added to spam email.	string	Maximum length: 63	Spam

### config smtp

Parameter	Description	Type	Size	Default
log-all	Enable/disable logging of all email traffic.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable logging of all email traffic.		
	<i>enable</i>	Enable logging of all email traffic.		

Parameter	Description	Type	Size	Default								
action	Action for spam email.	option	-	discard								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>pass</i></td><td>Allow spam email to pass through.</td></tr><tr><td><i>tag</i></td><td>Tag spam email with configured text in subject or header.</td></tr><tr><td><i>discard</i></td><td>Discard (block) spam email.</td></tr></table>	Option	Description	<i>pass</i>	Allow spam email to pass through.	<i>tag</i>	Tag spam email with configured text in subject or header.	<i>discard</i>	Discard (block) spam email.			
Option	Description											
<i>pass</i>	Allow spam email to pass through.											
<i>tag</i>	Tag spam email with configured text in subject or header.											
<i>discard</i>	Discard (block) spam email.											
tag-type	Tag subject or header for spam email.	option	-	subject spaminfo								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>subject</i></td><td>Prepend text to spam email subject.</td></tr><tr><td><i>header</i></td><td>Append a user defined mime header to spam email.</td></tr><tr><td><i>spaminfo</i></td><td>Append spam info to spam email header.</td></tr></table>	Option	Description	<i>subject</i>	Prepend text to spam email subject.	<i>header</i>	Append a user defined mime header to spam email.	<i>spaminfo</i>	Append spam info to spam email header.			
Option	Description											
<i>subject</i>	Prepend text to spam email subject.											
<i>header</i>	Append a user defined mime header to spam email.											
<i>spaminfo</i>	Append spam info to spam email header.											
tag-msg	Subject text or header added to spam email.	string	Maximum length: 63	Spam								
hdrip	Enable/disable SMTP email header IP checks for spamfsip, spamrbl, and spambal filters.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable SMTP email header IP checks for spamfsip, spamrbl, and spambal filters.</td></tr><tr><td><i>enable</i></td><td>Enable SMTP email header IP checks for spamfsip, spamrbl, and spambal filters.</td></tr></table>	Option	Description	<i>disable</i>	Disable SMTP email header IP checks for spamfsip, spamrbl, and spambal filters.	<i>enable</i>	Enable SMTP email header IP checks for spamfsip, spamrbl, and spambal filters.					
Option	Description											
<i>disable</i>	Disable SMTP email header IP checks for spamfsip, spamrbl, and spambal filters.											
<i>enable</i>	Enable SMTP email header IP checks for spamfsip, spamrbl, and spambal filters.											
local-override	Enable/disable local filter to override SMTP remote check result.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable local filter to override SMTP remote check result.</td></tr><tr><td><i>enable</i></td><td>Enable local filter to override SMTP remote check result.</td></tr></table>	Option	Description	<i>disable</i>	Disable local filter to override SMTP remote check result.	<i>enable</i>	Enable local filter to override SMTP remote check result.					
Option	Description											
<i>disable</i>	Disable local filter to override SMTP remote check result.											
<i>enable</i>	Enable local filter to override SMTP remote check result.											

### config yahoo-mail

Parameter	Description	Type	Size	Default
log-all	Enable/disable logging of all email traffic.	option	-	disable



Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable logging of all email traffic.		
	<i>enable</i>	Enable logging of all email traffic.		

## endpoint-control

This section includes syntax for the following commands:

- [config endpoint-control fctems on page 134](#)

### config endpoint-control fctems

Configure FortiClient Enterprise Management Server (EMS) entries.

```
config endpoint-control fctems
  Description: Configure FortiClient Enterprise Management Server (EMS) entries.
  edit <ems-id>
    set call-timeout {integer}
    set capabilities {option1}, {option2}, ...
    set cloud-server-type [production|alpha|...]
    set dirty-reason [none|mismatched-ems-sn]
    set fortinetone-cloud-authentication [enable|disable]
    set https-port {integer}
    set interface {string}
    set interface-select-method [auto|sdwan|...]
    set name {string}
    set out-of-sync-threshold {integer}
    set preserve-ssl-session [enable|disable]
    set pull-avatars [enable|disable]
    set pull-malware-hash [enable|disable]
    set pull-sysinfo [enable|disable]
    set pull-tags [enable|disable]
    set pull-vulnerabilities [enable|disable]
    set serial-number {string}
    set server {string}
    set source-ip {ipv4-address-any}
    set status [enable|disable]
    set trust-ca-cn [enable|disable]
    set websocket-override [disable|enable]
  next
end
```

### config endpoint-control fctems

Parameter	Description	Type	Size	Default
call-timeout	FortiClient EMS call timeout in seconds.	integer	Minimum value: 1 Maximum value: 180	30
capabilities	List of EMS capabilities.	option	-	

Parameter	Description	Type	Size	Default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>fabric-auth</i></td><td>Allow this FortiGate unit to load the authentication page provided by EMS to authenticate itself with EMS.</td></tr><tr><td><i>silent-approval</i></td><td>Allow silent approval of non-root or FortiGate HA clusters on EMS in the Security Fabric.</td></tr><tr><td><i>websocket</i></td><td>Enable/disable websockets for this FortiGate unit. Override behavior using websocket-override.</td></tr><tr><td><i>websocket-malware</i></td><td>Allow this FortiGate unit to request malware hash notifications over websocket.</td></tr><tr><td><i>push-ca-certs</i></td><td>Enable/disable syncing deep inspection certificates with EMS.</td></tr><tr><td><i>common-tags-api</i></td><td>Can receive tag information from New Common Tags API from EMS.</td></tr></table>	Option	Description	<i>fabric-auth</i>	Allow this FortiGate unit to load the authentication page provided by EMS to authenticate itself with EMS.	<i>silent-approval</i>	Allow silent approval of non-root or FortiGate HA clusters on EMS in the Security Fabric.	<i>websocket</i>	Enable/disable websockets for this FortiGate unit. Override behavior using websocket-override.	<i>websocket-malware</i>	Allow this FortiGate unit to request malware hash notifications over websocket.	<i>push-ca-certs</i>	Enable/disable syncing deep inspection certificates with EMS.	<i>common-tags-api</i>	Can receive tag information from New Common Tags API from EMS.			
	Option	Description																
	<i>fabric-auth</i>	Allow this FortiGate unit to load the authentication page provided by EMS to authenticate itself with EMS.																
	<i>silent-approval</i>	Allow silent approval of non-root or FortiGate HA clusters on EMS in the Security Fabric.																
	<i>websocket</i>	Enable/disable websockets for this FortiGate unit. Override behavior using websocket-override.																
	<i>websocket-malware</i>	Allow this FortiGate unit to request malware hash notifications over websocket.																
	<i>push-ca-certs</i>	Enable/disable syncing deep inspection certificates with EMS.																
<i>common-tags-api</i>	Can receive tag information from New Common Tags API from EMS.																	
cloud-server-type	Cloud server type.	option	-	production														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>production</i></td><td>Production FortiClient EMS Cloud Controller.</td></tr><tr><td><i>alpha</i></td><td>Alpha FortiClient EMS Cloud Controller. For testing only.</td></tr><tr><td><i>beta</i></td><td>Beta FortiClient EMS Cloud Controller. For testing only.</td></tr></table>	Option	Description	<i>production</i>	Production FortiClient EMS Cloud Controller.	<i>alpha</i>	Alpha FortiClient EMS Cloud Controller. For testing only.	<i>beta</i>	Beta FortiClient EMS Cloud Controller. For testing only.									
	Option	Description																
	<i>production</i>	Production FortiClient EMS Cloud Controller.																
	<i>alpha</i>	Alpha FortiClient EMS Cloud Controller. For testing only.																
<i>beta</i>	Beta FortiClient EMS Cloud Controller. For testing only.																	
dirty-reason	Dirty Reason for FortiClient EMS.	option	-	none														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>FortiClient EMS entry not dirty.</td></tr><tr><td><i>mismatched-ems-sn</i></td><td>FortiClient EMS entry dirty because EMS SN is mismatched with configured SN.</td></tr></table>	Option	Description	<i>none</i>	FortiClient EMS entry not dirty.	<i>mismatched-ems-sn</i>	FortiClient EMS entry dirty because EMS SN is mismatched with configured SN.											
	Option	Description																
	<i>none</i>	FortiClient EMS entry not dirty.																
<i>mismatched-ems-sn</i>	FortiClient EMS entry dirty because EMS SN is mismatched with configured SN.																	
ems-id	EMS ID in order	integer	Minimum value: 1 Maximum value: 5	0														
fortinetone-cloud-authentication	Enable/disable authentication of FortiClient EMS Cloud through FortiCloud account.	option	-	disable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable authentication of FortiClient EMS Cloud through the use of FortiCloud account.</td></tr></table>	Option	Description	<i>enable</i>	Enable authentication of FortiClient EMS Cloud through the use of FortiCloud account.													
	Option	Description																
<i>enable</i>	Enable authentication of FortiClient EMS Cloud through the use of FortiCloud account.																	

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable authentication of FortiClient EMS Cloud through the use of FortiCloud account.</td></tr></table>		Option	Description	<i>disable</i>	Disable authentication of FortiClient EMS Cloud through the use of FortiCloud account.						
	Option	Description										
<i>disable</i>	Disable authentication of FortiClient EMS Cloud through the use of FortiCloud account.											
https-port	FortiClient EMS HTTPS access port number..	integer	Minimum value: 1 Maximum value: 65535	443								
interface	Specify outgoing interface to reach server.	string	Maximum length: 15									
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto</i></td><td>Set outgoing interface automatically.</td></tr><tr><td><i>sdwan</i></td><td>Set outgoing interface by SD-WAN or policy routing rules.</td></tr><tr><td><i>specify</i></td><td>Set outgoing interface manually.</td></tr></table>		Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.		
	Option	Description										
	<i>auto</i>	Set outgoing interface automatically.										
	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.										
<i>specify</i>	Set outgoing interface manually.											
name	FortiClient Enterprise Management Server (EMS) name.	string	Maximum length: 35									
out-of-sync-threshold	Outdated resource threshold in seconds.	integer	Minimum value: 10 Maximum value: 3600	180								
preserve-ssl-session	Enable/disable preservation of EMS SSL session connection. Warning, most users should not touch this setting.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Allow preservation of EMS SSL session connection.</td></tr><tr><td><i>disable</i></td><td>Don't allow preservation of EMS SSL session connection.</td></tr></table>		Option	Description	<i>enable</i>	Allow preservation of EMS SSL session connection.	<i>disable</i>	Don't allow preservation of EMS SSL session connection.				
	Option	Description										
	<i>enable</i>	Allow preservation of EMS SSL session connection.										
<i>disable</i>	Don't allow preservation of EMS SSL session connection.											
pull-avatars	Enable/disable pulling avatars from EMS.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable pulling FortiClient user avatars from EMS.</td></tr><tr><td><i>disable</i></td><td>Disable pulling FortiClient user avatars from EMS.</td></tr></table>		Option	Description	<i>enable</i>	Enable pulling FortiClient user avatars from EMS.	<i>disable</i>	Disable pulling FortiClient user avatars from EMS.				
	Option	Description										
	<i>enable</i>	Enable pulling FortiClient user avatars from EMS.										
<i>disable</i>	Disable pulling FortiClient user avatars from EMS.											

Parameter	Description	Type	Size	Default						
pull-malware-hash	Enable/disable pulling FortiClient malware hash from EMS.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable pulling FortiClient malware hash from EMS.</td></tr><tr><td><i>disable</i></td><td>Disable pulling FortiClient malware hash from EMS.</td></tr></table>	Option	Description	<i>enable</i>	Enable pulling FortiClient malware hash from EMS.	<i>disable</i>	Disable pulling FortiClient malware hash from EMS.			
Option	Description									
<i>enable</i>	Enable pulling FortiClient malware hash from EMS.									
<i>disable</i>	Disable pulling FortiClient malware hash from EMS.									
pull-sysinfo	Enable/disable pulling SysInfo from EMS.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable pulling FortiClient user SysInfo from EMS.</td></tr><tr><td><i>disable</i></td><td>Disable pulling FortiClient user SysInfo from EMS.</td></tr></table>	Option	Description	<i>enable</i>	Enable pulling FortiClient user SysInfo from EMS.	<i>disable</i>	Disable pulling FortiClient user SysInfo from EMS.			
Option	Description									
<i>enable</i>	Enable pulling FortiClient user SysInfo from EMS.									
<i>disable</i>	Disable pulling FortiClient user SysInfo from EMS.									
pull-tags	Enable/disable pulling FortiClient user tags from EMS.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable pulling FortiClient user tags from EMS.</td></tr><tr><td><i>disable</i></td><td>Disable pulling FortiClient user tags from EMS.</td></tr></table>	Option	Description	<i>enable</i>	Enable pulling FortiClient user tags from EMS.	<i>disable</i>	Disable pulling FortiClient user tags from EMS.			
Option	Description									
<i>enable</i>	Enable pulling FortiClient user tags from EMS.									
<i>disable</i>	Disable pulling FortiClient user tags from EMS.									
pull-vulnerabilities	Enable/disable pulling vulnerabilities from EMS.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable pulling client vulnerabilities from EMS.</td></tr><tr><td><i>disable</i></td><td>Disable pulling client vulnerabilities from EMS.</td></tr></table>	Option	Description	<i>enable</i>	Enable pulling client vulnerabilities from EMS.	<i>disable</i>	Disable pulling client vulnerabilities from EMS.			
Option	Description									
<i>enable</i>	Enable pulling client vulnerabilities from EMS.									
<i>disable</i>	Disable pulling client vulnerabilities from EMS.									
serial-number	EMS Serial Number.	string	Maximum length: 16							
server	FortiClient EMS FQDN or IPv4 address.	string	Maximum length: 255							
source-ip	REST API call source IP.	ipv4-address-any	Not Specified	0.0.0.0						
status	Enable or disable this EMS configuration.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable EMS configuration and operation.</td></tr><tr><td><i>disable</i></td><td>Disable EMS configuration and operation.</td></tr></table>	Option	Description	<i>enable</i>	Enable EMS configuration and operation.	<i>disable</i>	Disable EMS configuration and operation.			
Option	Description									
<i>enable</i>	Enable EMS configuration and operation.									
<i>disable</i>	Disable EMS configuration and operation.									

Parameter	Description	Type	Size	Default						
trust-ca-cn	Enable/disable trust of the EMS certificate issuer (CA) and common name(CN) for certificate auto-renewal.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Trust EMS certificate CA &amp; CN to automatically renew certificate.</td></tr><tr><td><i>disable</i></td><td>Do not trust EMS certificate CA &amp; CN to automatically renew certificate.</td></tr></table>				Option	Description	<i>enable</i>	Trust EMS certificate CA & CN to automatically renew certificate.	<i>disable</i>	Do not trust EMS certificate CA & CN to automatically renew certificate.
Option	Description									
<i>enable</i>	Trust EMS certificate CA & CN to automatically renew certificate.									
<i>disable</i>	Do not trust EMS certificate CA & CN to automatically renew certificate.									
websocket-override	Enable/disable override behavior for how this FortiGate unit connects to EMS using a WebSocket connection.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Do not override the WebSocket connection. Connect to WebSocket of this EMS server if it is capable (default).</td></tr><tr><td><i>enable</i></td><td>Override the WebSocket connection. Do not connect to WebSocket even if EMS is capable of a WebSocket connection.</td></tr></table>				Option	Description	<i>disable</i>	Do not override the WebSocket connection. Connect to WebSocket of this EMS server if it is capable (default).	<i>enable</i>	Override the WebSocket connection. Do not connect to WebSocket even if EMS is capable of a WebSocket connection.
Option	Description									
<i>disable</i>	Do not override the WebSocket connection. Connect to WebSocket of this EMS server if it is capable (default).									
<i>enable</i>	Override the WebSocket connection. Do not connect to WebSocket even if EMS is capable of a WebSocket connection.									

## extender-controller

This section includes syntax for the following commands:

- [config extender-controller dataplan on page 139](#)
- [config extender-controller extender-profile on page 142](#)
- [config extender-controller extender on page 153](#)

### config extender-controller dataplan

FortiExtender dataplan configuration.

```
config extender-controller dataplan
  Description: FortiExtender dataplan configuration.
  edit <name>
    set apn {string}
    set auth-type [none|pap|...]
    set billing-date {integer}
    set capacity {integer}
    set carrier {string}
    set iccid {string}
    set modem-id [modem1|modem2|...]
    set monthly-fee {integer}
    set overage [disable|enable]
    set password {password}
    set pdn [ipv4-only|ipv6-only|...]
    set preferred-subnet {integer}
    set private-network [disable|enable]
    set signal-period {integer}
    set signal-threshold {integer}
    set slot [sim1|sim2]
    set type [carrier|slot|...]
    set username {string}
  next
end
```

### config extender-controller dataplan

Parameter	Description	Type	Size	Default
apn	APN configuration.	string	Maximum length: 63	
auth-type	Authentication type.	option	-	none

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>No authentication.</td></tr><tr><td><i>pap</i></td><td>PAP.</td></tr><tr><td><i>chap</i></td><td>CHAP.</td></tr></table>	Option	Description	<i>none</i>	No authentication.	<i>pap</i>	PAP.	<i>chap</i>	CHAP.			
	Option	Description										
	<i>none</i>	No authentication.										
	<i>pap</i>	PAP.										
<i>chap</i>	CHAP.											
billing-date	Billing day of the month.	integer	Minimum value: 1 Maximum value: 31	1								
capacity	Capacity in MB.	integer	Minimum value: 0 Maximum value: 102400000	0								
carrier	Carrier configuration.	string	Maximum length: 31									
iccid	ICCID configuration.	string	Maximum length: 31									
modem-id	Dataplan's modem specifics, if any.	option	-	all								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>modem1</i></td><td>Modem one.</td></tr><tr><td><i>modem2</i></td><td>Modem two.</td></tr><tr><td><i>all</i></td><td>All modems.</td></tr></table>	Option	Description	<i>modem1</i>	Modem one.	<i>modem2</i>	Modem two.	<i>all</i>	All modems.			
	Option	Description										
	<i>modem1</i>	Modem one.										
	<i>modem2</i>	Modem two.										
<i>all</i>	All modems.											
monthly-fee	Monthly fee of dataplan.	integer	Minimum value: 0 Maximum value: 1000000	0								
name	FortiExtender data plan name.	string	Maximum length: 31									
overage	Enable/disable dataplan overage detection.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable dataplan overage detection.</td></tr><tr><td><i>enable</i></td><td>Enable dataplan overage detection.</td></tr></table>	Option	Description	<i>disable</i>	Disable dataplan overage detection.	<i>enable</i>	Enable dataplan overage detection.					
	Option	Description										
	<i>disable</i>	Disable dataplan overage detection.										
<i>enable</i>	Enable dataplan overage detection.											
password	Password.	password	Not Specified									



Parameter	Description	Type	Size	Default										
pdn	PDN type.	option	-	ipv4-only										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ipv4-only</td><td>IPv4 only PDN activation.</td></tr><tr><td>ipv6-only</td><td>IPv6 only PDN activation.</td></tr><tr><td>ipv4-ipv6</td><td>Both IPv4 and IPv6 PDN activations.</td></tr></table>	Option	Description	ipv4-only	IPv4 only PDN activation.	ipv6-only	IPv6 only PDN activation.	ipv4-ipv6	Both IPv4 and IPv6 PDN activations.					
Option	Description													
ipv4-only	IPv4 only PDN activation.													
ipv6-only	IPv6 only PDN activation.													
ipv4-ipv6	Both IPv4 and IPv6 PDN activations.													
preferred-subnet	Preferred subnet mask.	integer	Minimum value: 0 Maximum value: 32	0										
private-network	Enable/disable dataplan private network support.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable dataplan private network support.</td></tr><tr><td>enable</td><td>Enable dataplan private network support.</td></tr></table>	Option	Description	disable	Disable dataplan private network support.	enable	Enable dataplan private network support.							
Option	Description													
disable	Disable dataplan private network support.													
enable	Enable dataplan private network support.													
signal-period	Signal period (600 to 18000 seconds).	integer	Minimum value: 600 Maximum value: 18000	3600										
signal-threshold	Signal threshold. Specify the range between 50 - 100, where 50/100 means -50/-100 dBm.	integer	Minimum value: 50 Maximum value: 100	100										
slot	SIM slot configuration.	option	-											
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>sim1</td><td>Sim slot one.</td></tr><tr><td>sim2</td><td>Sim slot two.</td></tr></table>	Option	Description	sim1	Sim slot one.	sim2	Sim slot two.							
Option	Description													
sim1	Sim slot one.													
sim2	Sim slot two.													
type	Type preferences configuration.	option	-	generic										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>carrier</td><td>Assign by SIM carrier.</td></tr><tr><td>slot</td><td>Assign to SIM slot 1 or 2.</td></tr><tr><td>iccid</td><td>Assign to a specific SIM by ICCID.</td></tr><tr><td>generic</td><td>Compatible with any SIM. Assigned if no other dataplan matches the chosen SIM.</td></tr></table>	Option	Description	carrier	Assign by SIM carrier.	slot	Assign to SIM slot 1 or 2.	iccid	Assign to a specific SIM by ICCID.	generic	Compatible with any SIM. Assigned if no other dataplan matches the chosen SIM.			
Option	Description													
carrier	Assign by SIM carrier.													
slot	Assign to SIM slot 1 or 2.													
iccid	Assign to a specific SIM by ICCID.													
generic	Compatible with any SIM. Assigned if no other dataplan matches the chosen SIM.													

Parameter	Description	Type	Size	Default
username	Username.	string	Maximum length: 127	

## config extender-controller extender-profile

FortiExtender extender profile configuration.

```

config extender-controller extender-profile
    Description: FortiExtender extender profile configuration.
    edit <name>
        set allowaccess {option1}, {option2}, ...
        set bandwidth-limit {integer}
        config cellular
            Description: FortiExtender cellular configuration.
            set dataplan <name1>, <name2>, ...
            config controller-report
                Description: FortiExtender controller report configuration.
                set status [disable|enable]
                set interval {integer}
                set signal-threshold {integer}
            end
            config sms-notification
                Description: FortiExtender cellular SMS notification configuration.
                set status [disable|enable]
                config alert
                    Description: SMS alert list.
                    set system-reboot {string}
                    set data-exhausted {string}
                    set session-disconnect {string}
                    set low-signal-strength {string}
                    set os-image-fallback {string}
                    set mode-switch {string}
                    set fgt-backup-mode-switch {string}
                end
                config receiver
                    Description: SMS notification receiver list.
                    edit <name>
                        set status [disable|enable]
                        set phone-number {string}
                        set alert {option1}, {option2}, ...
                    next
                end
            end
        end
    config modem1
        Description: Configuration options for modem 1.
        set redundant-mode [disable|enable]
        set redundant-intf {string}
        set conn-status {integer}
        set default-sim [sim1|sim2|...]
        set gps [disable|enable]
        set sim1-pin [disable|enable]
        set sim2-pin [disable|enable]
    
```

```

set sim1-pin-code {password}
set sim2-pin-code {password}
set preferred-carrier {string}
config auto-switch
    Description: FortiExtender auto switch configuration.
    set disconnect [disable|enable]
    set disconnect-threshold {integer}
    set disconnect-period {integer}
    set signal [disable|enable]
    set dataplan [disable|enable]
    set switch-back {option1}, {option2}, ...
    set switch-back-time {string}
    set switch-back-timer {integer}
end
end
config modem2
    Description: Configuration options for modem 2.
    set redundant-mode [disable|enable]
    set redundant-intf {string}
    set conn-status {integer}
    set default-sim [sim1|sim2|...]
    set gps [disable|enable]
    set sim1-pin [disable|enable]
    set sim2-pin [disable|enable]
    set sim1-pin-code {password}
    set sim2-pin-code {password}
    set preferred-carrier {string}
    config auto-switch
        Description: FortiExtender auto switch configuration.
        set disconnect [disable|enable]
        set disconnect-threshold {integer}
        set disconnect-period {integer}
        set signal [disable|enable]
        set dataplan [disable|enable]
        set switch-back {option1}, {option2}, ...
        set switch-back-time {string}
        set switch-back-timer {integer}
    end
end
end
set enforce-bandwidth [enable|disable]
set extension [wan-extension|lan-extension]
set id {integer}
config lan-extension
    Description: FortiExtender lan extension configuration.
    set link-loadbalance [activebackup|loadbalance]
    set ipsec-tunnel {string}
    set backhaul-interface {string}
    set backhaul-ip {string}
    config backhaul
        Description: LAN extension backhaul tunnel configuration.
        edit <name>
            set port [wan|lte1|...]
            set role [primary|secondary]
            set weight {integer}
        next
    end
end

```

```

        end
    end
    set login-password {password}
    set login-password-change [yes|default|...]
    set model [FX201E|FX211E|...]
next
end

```

## config extender-controller extender-profile

Parameter	Description	Type	Size	Default														
allowaccess	Control management access to the managed extender. Separate entries with a space.	option	-															
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ping</i></td><td>PING access.</td></tr><tr><td><i>telnet</i></td><td>TELNET access.</td></tr><tr><td><i>http</i></td><td>HTTP access.</td></tr><tr><td><i>https</i></td><td>HTTPS access.</td></tr><tr><td><i>ssh</i></td><td>SSH access.</td></tr><tr><td><i>snmp</i></td><td>SNMP access.</td></tr></table>	Option	Description	<i>ping</i>	PING access.	<i>telnet</i>	TELNET access.	<i>http</i>	HTTP access.	<i>https</i>	HTTPS access.	<i>ssh</i>	SSH access.	<i>snmp</i>	SNMP access.			
Option	Description																	
<i>ping</i>	PING access.																	
<i>telnet</i>	TELNET access.																	
<i>http</i>	HTTP access.																	
<i>https</i>	HTTPS access.																	
<i>ssh</i>	SSH access.																	
<i>snmp</i>	SNMP access.																	
bandwidth-limit	FortiExtender LAN extension bandwidth limit (Mbps).	integer	Minimum value: 1 Maximum value: 16776000	1024														
enforce-bandwidth	Enable/disable enforcement of bandwidth on LAN extension interface.	option	-	disable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable to enforce bandwidth limit on LAN extension interface.</td></tr><tr><td><i>disable</i></td><td>Disable to enforce bandwidth limit on LAN extension interface.</td></tr></table>	Option	Description	<i>enable</i>	Enable to enforce bandwidth limit on LAN extension interface.	<i>disable</i>	Disable to enforce bandwidth limit on LAN extension interface.											
Option	Description																	
<i>enable</i>	Enable to enforce bandwidth limit on LAN extension interface.																	
<i>disable</i>	Disable to enforce bandwidth limit on LAN extension interface.																	
extension	Extension option.	option	-	wan-extension														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>wan-extension</i></td><td>WAN extension.</td></tr><tr><td><i>lan-extension</i></td><td>LAN extension.</td></tr></table>	Option	Description	<i>wan-extension</i>	WAN extension.	<i>lan-extension</i>	LAN extension.											
Option	Description																	
<i>wan-extension</i>	WAN extension.																	
<i>lan-extension</i>	LAN extension.																	

Parameter	Description	Type	Size	Default																														
id	ID.	integer	Minimum value: 0 Maximum value: 102400000	32																														
login-password	Set the managed extender's administrator password.	password	Not Specified																															
login-password-change	Change or reset the administrator password of a managed extender.	option	-	no																														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>yes</td><td>Change the managed extender's administrator password. Use the login-password option to set the password.</td></tr><tr><td>default</td><td>Keep the managed extender's administrator password set to the factory default.</td></tr><tr><td>no</td><td>Do not change the managed extender's administrator password.</td></tr></table>				Option	Description	yes	Change the managed extender's administrator password. Use the login-password option to set the password.	default	Keep the managed extender's administrator password set to the factory default.	no	Do not change the managed extender's administrator password.																						
	Option	Description																																
	yes	Change the managed extender's administrator password. Use the login-password option to set the password.																																
	default	Keep the managed extender's administrator password set to the factory default.																																
no	Do not change the managed extender's administrator password.																																	
model	Model.	option	-	FX201E																														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>FX201E</td><td>FEX-201E model.</td></tr><tr><td>FX211E</td><td>FEX-211E model.</td></tr><tr><td>FX200F</td><td>FEX-200F model.</td></tr><tr><td>FXA11F</td><td>FEX-101F-AM model.</td></tr><tr><td>FXE11F</td><td>FEX-101F-EA model.</td></tr><tr><td>FXA21F</td><td>FEX-201F-AM model.</td></tr><tr><td>FXE21F</td><td>FEX-201F-EA model.</td></tr><tr><td>FXA22F</td><td>FEX-202F-AM model.</td></tr><tr><td>FXE22F</td><td>FEX-202F-EA model.</td></tr><tr><td>FX212F</td><td>FEX-212F model.</td></tr><tr><td>FX311F</td><td>FEX-311F model.</td></tr><tr><td>FX312F</td><td>FEX-312F model.</td></tr><tr><td>FX511F</td><td>FEX-511F model.</td></tr><tr><td>FVG21F</td><td>FEV-211F model.</td></tr></table>				Option	Description	FX201E	FEX-201E model.	FX211E	FEX-211E model.	FX200F	FEX-200F model.	FXA11F	FEX-101F-AM model.	FXE11F	FEX-101F-EA model.	FXA21F	FEX-201F-AM model.	FXE21F	FEX-201F-EA model.	FXA22F	FEX-202F-AM model.	FXE22F	FEX-202F-EA model.	FX212F	FEX-212F model.	FX311F	FEX-311F model.	FX312F	FEX-312F model.	FX511F	FEX-511F model.	FVG21F	FEV-211F model.
	Option	Description																																
	FX201E	FEX-201E model.																																
	FX211E	FEX-211E model.																																
	FX200F	FEX-200F model.																																
	FXA11F	FEX-101F-AM model.																																
	FXE11F	FEX-101F-EA model.																																
	FXA21F	FEX-201F-AM model.																																
	FXE21F	FEX-201F-EA model.																																
	FXA22F	FEX-202F-AM model.																																
	FXE22F	FEX-202F-EA model.																																
	FX212F	FEX-212F model.																																
	FX311F	FEX-311F model.																																
	FX312F	FEX-312F model.																																
	FX511F	FEX-511F model.																																
FVG21F	FEV-211F model.																																	

Parameter	Description	Type	Size	Default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>FVA21F</i></td><td>FEV-211F-AM model.</td></tr><tr><td><i>FVG22F</i></td><td>FEV-212F model.</td></tr><tr><td><i>FVA22F</i></td><td>FEV-212F-AM model.</td></tr><tr><td><i>FX04DA</i></td><td>FX40D-AMEU model.</td></tr><tr><td><i>FX04DN</i></td><td>FX40D-NAM model,</td></tr><tr><td><i>FX04DI</i></td><td>FX40D-INTL model,</td></tr></table>	Option	Description	<i>FVA21F</i>	FEV-211F-AM model.	<i>FVG22F</i>	FEV-212F model.	<i>FVA22F</i>	FEV-212F-AM model.	<i>FX04DA</i>	FX40D-AMEU model.	<i>FX04DN</i>	FX40D-NAM model,	<i>FX04DI</i>	FX40D-INTL model,			
	Option	Description																
	<i>FVA21F</i>	FEV-211F-AM model.																
	<i>FVG22F</i>	FEV-212F model.																
	<i>FVA22F</i>	FEV-212F-AM model.																
	<i>FX04DA</i>	FX40D-AMEU model.																
	<i>FX04DN</i>	FX40D-NAM model,																
<i>FX04DI</i>	FX40D-INTL model,																	
name	FortiExtender profile name.	string	Maximum length: 31															

### config cellular

Parameter	Description	Type	Size	Default
dataplan <name>	Dataplan names. Dataplan name.	string	Maximum length: 79	

### config controller-report

Parameter	Description	Type	Size	Default						
status	FortiExtender controller report status.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Controller is configured to not provide service to this FortiExtender.</td></tr><tr><td><i>enable</i></td><td>Controller is configured to provide service to this FortiExtender.</td></tr></table>	Option	Description	<i>disable</i>	Controller is configured to not provide service to this FortiExtender.	<i>enable</i>	Controller is configured to provide service to this FortiExtender.			
	Option	Description								
	<i>disable</i>	Controller is configured to not provide service to this FortiExtender.								
<i>enable</i>	Controller is configured to provide service to this FortiExtender.									
interval	Controller report interval.	integer	Minimum value: 0 Maximum value: 4294967295	300						
signal-threshold	Controller report signal threshold.	integer	Minimum value: 10 Maximum value: 50	10						

### config sms-notification

Parameter	Description	Type	Size	Default
status	FortiExtender SMS notification status.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	SMS notification is configured to not provide service to this FortiExtender.		
	<i>enable</i>	SMS notification is configured to provide service to this FortiExtender.		

### config alert

Parameter	Description	Type	Size	Default
system-reboot	Display string when system rebooted.	string	Maximum length: 63	system will reboot
data-exhausted	Display string when data exhausted.	string	Maximum length: 63	data plan is exhausted
session-disconnect	Display string when session disconnected.	string	Maximum length: 63	LTE data session is disconnected
low-signal-strength	Display string when signal strength is low.	string	Maximum length: 63	LTE signal strength is too low
os-image-fallback	Display string when falling back to a previous OS image.	string	Maximum length: 63	system start to fallback OS image
mode-switch	Display string when mode is switched.	string	Maximum length: 63	system networking mode switched
fgt-backup-mode-switch	Display string when FortiGate backup mode switched.	string	Maximum length: 63	FortiGate backup work mode switched

### config receiver

Parameter	Description	Type	Size	Default
name	FortiExtender SMS notification receiver name.	string	Maximum length: 31	
status	SMS notification receiver status.	option	-	disable

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable SMS notification receiver.		
	<i>enable</i>	Enable SMS notification receiver.		
phone-number	Receiver phone number. Format: [+][country code][area code][local phone number]. For example, +16501234567.	string	Maximum length: 31	
alert	Alert multi-options.	option	-	
	<b>Option</b>	<b>Description</b>		
	<i>system-reboot</i>	System will reboot.		
	<i>data-exhausted</i>	Data plan is exhausted.		
	<i>session-disconnect</i>	LTE data session is disconnected.		
	<i>low-signal-strength</i>	LTE signal strength is too low.		
	<i>mode-switch</i>	System is starting to use fallback OS image.		
	<i>os-image-fallback</i>	System networking mode switched.		
	<i>fgt-backup-mode-switch</i>	FortiGate backup work mode switched.		

### config modem1

Parameter	Description	Type	Size	Default
redundant-mode	FortiExtender mode.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable interface redundancy.		
	<i>enable</i>	Enable interface redundancy.		
redundant-intf	Redundant interface.	string	Maximum length: 15	
conn-status	Connection status.	integer	Minimum value: 0 Maximum value: 4294967295	0



Parameter	Description	Type	Size	Default
default-sim	Default SIM selection.	option	-	sim1
	<b>Option</b>	<b>Description</b>		
	<i>sim1</i>	Use SIM #1 by default.		
	<i>sim2</i>	Use SIM #2 by default.		
	<i>carrier</i>	Assign default SIM based on carrier.		
	<i>cost</i>	Assign default SIM based on cost.		
gps	FortiExtender GPS enable/disable.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable GPS.		
	<i>enable</i>	Enable GPS.		
sim1-pin	SIM #1 PIN status.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable SIM #1 PIN.		
	<i>enable</i>	Enable SIM #1 PIN.		
sim2-pin	SIM #2 PIN status.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable SIM #2 PIN.		
	<i>enable</i>	Enable SIM #2 PIN.		
sim1-pin-code	SIM #1 PIN password.	password	Not Specified	
sim2-pin-code	SIM #2 PIN password.	password	Not Specified	
preferred-carrier	Preferred carrier.	string	Maximum length: 31	

#### config auto-switch

Parameter	Description	Type	Size	Default
disconnect	Auto switch by disconnect.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable switching of SIM card based on cellular disconnections.		
	<i>enable</i>	Enable switching of SIM card based on cellular disconnections.		

Parameter	Description	Type	Size	Default						
disconnect-threshold	Automatically switch based on disconnect threshold.	integer	Minimum value: 1 Maximum value: 100	3						
disconnect-period	Automatically switch based on disconnect period.	integer	Minimum value: 600 Maximum value: 18000	600						
signal	Automatically switch based on signal strength.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable switching of SIM card based on cellular signal quality.</td></tr><tr><td>enable</td><td>Enable switching of SIM card based on cellular signal quality.</td></tr></table>				Option	Description	disable	Disable switching of SIM card based on cellular signal quality.	enable	Enable switching of SIM card based on cellular signal quality.
Option	Description									
disable	Disable switching of SIM card based on cellular signal quality.									
enable	Enable switching of SIM card based on cellular signal quality.									
dataplan	Automatically switch based on data usage.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable switching of SIM card based on cellular data usage.</td></tr><tr><td>enable</td><td>Enable switching of SIM card based on cellular data usage.</td></tr></table>				Option	Description	disable	Disable switching of SIM card based on cellular data usage.	enable	Enable switching of SIM card based on cellular data usage.
Option	Description									
disable	Disable switching of SIM card based on cellular data usage.									
enable	Enable switching of SIM card based on cellular data usage.									
switch-back	Auto switch with switch back multi-options.	option	-							
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>time</td><td>Switch back based on specific time in UTC (HH:MM).</td></tr><tr><td>timer</td><td>Switch back based on an interval.</td></tr></table>				Option	Description	time	Switch back based on specific time in UTC (HH:MM).	timer	Switch back based on an interval.
Option	Description									
time	Switch back based on specific time in UTC (HH:MM).									
timer	Switch back based on an interval.									
switch-back-time	Automatically switch over to preferred SIM/carrier at a specified time in UTC (HH:MM).	string	Maximum length: 31	00:01						
switch-back-timer	Automatically switch over to preferred SIM/carrier after the given time.	integer	Minimum value: 3600 Maximum value: 2147483647	86400						

## config modem2

Parameter	Description	Type	Size	Default
redundant-mode	FortiExtender mode.	option	-	disable

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable interface redundancy.		
	<i>enable</i>	Enable interface redundancy.		
redundant-intf	Redundant interface.	string	Maximum length: 15	
conn-status	Connection status.	integer	Minimum value: 0 Maximum value: 4294967295	0
default-sim	Default SIM selection.	option	-	sim1
	<b>Option</b>	<b>Description</b>		
	<i>sim1</i>	Use SIM #1 by default.		
	<i>sim2</i>	Use SIM #2 by default.		
	<i>carrier</i>	Assign default SIM based on carrier.		
	<i>cost</i>	Assign default SIM based on cost.		
gps	FortiExtender GPS enable/disable.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable GPS.		
	<i>enable</i>	Enable GPS.		
sim1-pin	SIM #1 PIN status.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable SIM #1 PIN.		
	<i>enable</i>	Enable SIM #1 PIN.		
sim2-pin	SIM #2 PIN status.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable SIM #2 PIN.		
	<i>enable</i>	Enable SIM #2 PIN.		
sim1-pin-code	SIM #1 PIN password.	password	Not Specified	
sim2-pin-code	SIM #2 PIN password.	password	Not Specified	

Parameter	Description	Type	Size	Default
preferred-carrier	Preferred carrier.	string	Maximum length: 31	

### config auto-switch

Parameter	Description	Type	Size	Default
disconnect	Auto switch by disconnect.	option	-	disable
disconnect-threshold	Automatically switch based on disconnect threshold.	integer	Minimum value: 1 Maximum value: 100	3
disconnect-period	Automatically switch based on disconnect period.	integer	Minimum value: 600 Maximum value: 18000	600
signal	Automatically switch based on signal strength.	option	-	disable
dataplan	Automatically switch based on data usage.	option	-	disable
switch-back	Auto switch with switch back multi-options.	option	-	
switch-back-time	Automatically switch over to preferred SIM/carrier at a specified time in UTC (HH:MM).	string	Maximum length: 31	00:01
switch-back-timer	Automatically switch over to preferred SIM/carrier after the given time.	integer	Minimum value: 3600 Maximum value: 2147483647	86400

### config lan-extension

Parameter	Description	Type	Size	Default
link-loadbalance	LAN extension link load balance strategy.	option	-	activebackup
	<b>Option</b>	<b>Description</b>		
	<i>activebackup</i>	FortiExtender LAN extension active-backup.		
	<i>loadbalance</i>	FortiExtender LAN extension load-balance.		
ipsec-tunnel	IPsec tunnel name.	string	Maximum length: 15	

Parameter	Description	Type	Size	Default
backhaul-interface	IPsec phase1 interface.	string	Maximum length: 15	
backhaul-ip	IPsec phase1 IPv4/FQDN. Used to specify the external IP/FQDN when the FortiGate unit is behind a NAT device.	string	Maximum length: 63	

### config backhaul

Parameter	Description	Type	Size	Default																				
name	FortiExtender LAN extension backhaul name.	string	Maximum length: 31																					
port	FortiExtender uplink port.	option	-	wan																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>wan</td><td>FortiExtender WAN port.</td></tr><tr><td>lte1</td><td>FortiExtender LTE1 port.</td></tr><tr><td>lte2</td><td>FortiExtender LTE2 port.</td></tr><tr><td>port1</td><td>FortiExtender port1 port.</td></tr><tr><td>port2</td><td>FortiExtender port2 port.</td></tr><tr><td>port3</td><td>FortiExtender port3 port.</td></tr><tr><td>port4</td><td>FortiExtender port4 port.</td></tr><tr><td>port5</td><td>FortiExtender port5 port.</td></tr><tr><td>sfp</td><td>FortiExtender SFP port.</td></tr></table>				Option	Description	wan	FortiExtender WAN port.	lte1	FortiExtender LTE1 port.	lte2	FortiExtender LTE2 port.	port1	FortiExtender port1 port.	port2	FortiExtender port2 port.	port3	FortiExtender port3 port.	port4	FortiExtender port4 port.	port5	FortiExtender port5 port.	sfp	FortiExtender SFP port.
	Option	Description																						
	wan	FortiExtender WAN port.																						
	lte1	FortiExtender LTE1 port.																						
	lte2	FortiExtender LTE2 port.																						
	port1	FortiExtender port1 port.																						
	port2	FortiExtender port2 port.																						
	port3	FortiExtender port3 port.																						
	port4	FortiExtender port4 port.																						
	port5	FortiExtender port5 port.																						
sfp	FortiExtender SFP port.																							
role	FortiExtender uplink port.	option	-	primary																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>primary</td><td>FortiExtender LAN extension primary role.</td></tr><tr><td>secondary</td><td>FortiExtender LAN extension secondary role.</td></tr></table>				Option	Description	primary	FortiExtender LAN extension primary role.	secondary	FortiExtender LAN extension secondary role.														
	Option	Description																						
	primary	FortiExtender LAN extension primary role.																						
secondary	FortiExtender LAN extension secondary role.																							
weight	WRR weight parameter.	integer	Minimum value: 1 Maximum value: 256	1																				

### config extender-controller extender

Extender controller configuration.

```

config extender-controller extender
    Description: Extender controller configuration.
    edit <name>
        set allowaccess {option1}, {option2}, ...
        set authorized [disable|enable]
        set bandwidth-limit {integer}
        set description {string}
        set device-id {integer}
        set enforce-bandwidth [enable|disable]
        set ext-name {string}
        set extension-type [wan-extension|lan-extension]
        set id {string}
        set login-password {password}
        set login-password-change [yes|default|...]
        set override-allowaccess [enable|disable]
        set override-enforce-bandwidth [enable|disable]
        set override-login-password-change [enable|disable]
        set profile {string}
        set vdom {integer}
        config wan-extension
            Description: FortiExtender wan extension configuration.
            set modem1-extension {string}
            set modem2-extension {string}
        end
    end
next
end

```

## config extender-controller extender

Parameter	Description	Type	Size	Default														
allowaccess	Control management access to the managed extender. Separate entries with a space.	option	-															
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ping</i></td><td>PING access.</td></tr><tr><td><i>telnet</i></td><td>TELNET access.</td></tr><tr><td><i>http</i></td><td>HTTP access.</td></tr><tr><td><i>https</i></td><td>HTTPS access.</td></tr><tr><td><i>ssh</i></td><td>SSH access.</td></tr><tr><td><i>snmp</i></td><td>SNMP access.</td></tr></table>	Option	Description	<i>ping</i>	PING access.	<i>telnet</i>	TELNET access.	<i>http</i>	HTTP access.	<i>https</i>	HTTPS access.	<i>ssh</i>	SSH access.	<i>snmp</i>	SNMP access.			
Option	Description																	
<i>ping</i>	PING access.																	
<i>telnet</i>	TELNET access.																	
<i>http</i>	HTTP access.																	
<i>https</i>	HTTPS access.																	
<i>ssh</i>	SSH access.																	
<i>snmp</i>	SNMP access.																	
authorized	FortiExtender Administration (enable or disable).	option	-	disable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Controller is configured to not provide service to this FortiExtender.</td></tr><tr><td><i>enable</i></td><td>Controller is configured to provide service to this FortiExtender.</td></tr></table>	Option	Description	<i>disable</i>	Controller is configured to not provide service to this FortiExtender.	<i>enable</i>	Controller is configured to provide service to this FortiExtender.											
Option	Description																	
<i>disable</i>	Controller is configured to not provide service to this FortiExtender.																	
<i>enable</i>	Controller is configured to provide service to this FortiExtender.																	

Parameter	Description	Type	Size	Default						
bandwidth-limit	FortiExtender LAN extension bandwidth limit (Mbps).	integer	Minimum value: 1 Maximum value: 16776000	1024						
description	Description.	string	Maximum length: 255							
device-id	Device ID.	integer	Minimum value: 0 Maximum value: 4294967295	1024						
enforce-bandwidth	Enable/disable enforcement of bandwidth on LAN extension interface.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable to enforce bandwidth limit on LAN extension interface.</td></tr><tr><td><i>disable</i></td><td>Disable to enforce bandwidth limit on LAN extension interface.</td></tr></table>				Option	Description	<i>enable</i>	Enable to enforce bandwidth limit on LAN extension interface.	<i>disable</i>	Disable to enforce bandwidth limit on LAN extension interface.
Option	Description									
<i>enable</i>	Enable to enforce bandwidth limit on LAN extension interface.									
<i>disable</i>	Disable to enforce bandwidth limit on LAN extension interface.									
ext-name	FortiExtender name.	string	Maximum length: 31							
extension-type	Extension type for this FortiExtender.	option	-							
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>wan-extension</i></td><td>FortiExtender wan-extension.</td></tr><tr><td><i>lan-extension</i></td><td>FortiExtender lan-extension.</td></tr></table>				Option	Description	<i>wan-extension</i>	FortiExtender wan-extension.	<i>lan-extension</i>	FortiExtender lan-extension.
Option	Description									
<i>wan-extension</i>	FortiExtender wan-extension.									
<i>lan-extension</i>	FortiExtender lan-extension.									
id	FortiExtender serial number.	string	Maximum length: 19							
login-password	Set the managed extender's administrator password.	password	Not Specified							
login-password-change	Change or reset the administrator password of a managed extender.	option	-	no						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>yes</i></td><td>Change the managed extender's administrator password. Use the login-password option to set the password.</td></tr><tr><td><i>default</i></td><td>Keep the managed extender's administrator password set to the factory default.</td></tr></table>				Option	Description	<i>yes</i>	Change the managed extender's administrator password. Use the login-password option to set the password.	<i>default</i>	Keep the managed extender's administrator password set to the factory default.
Option	Description									
<i>yes</i>	Change the managed extender's administrator password. Use the login-password option to set the password.									
<i>default</i>	Keep the managed extender's administrator password set to the factory default.									

Parameter	Description	Type	Size	Default
	<b>Option</b> <b>Description</b>			
	<i>no</i>	Do not change the managed extender's administrator password.		
name	FortiExtender entry name.	string	Maximum length: 19	
override-allowaccess	Enable to override the extender profile management access configuration.	option	-	disable
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Override the extender profile management access configuration.		
	<i>disable</i>	Use the extender profile management access configuration.		
override-enforce-bandwidth	Enable to override the extender profile enforce-bandwidth setting.	option	-	disable
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Enable override of FortiExtender profile bandwidth setting.		
	<i>disable</i>	Disable override of FortiExtender profile bandwidth setting.		
override-login-password-change	Enable to override the extender profile login-password (administrator password) setting.	option	-	disable
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Override the WTP profile login-password (administrator password) setting.		
	<i>disable</i>	Use the the WTP profile login-password (administrator password) setting.		
profile	FortiExtender profile configuration.	string	Maximum length: 31	
vdom	VDOM.	integer	Minimum value: 0 Maximum value: 4294967295	0

### config wan-extension

Parameter	Description	Type	Size	Default
modem1-extension	FortiExtender interface name.	string	Maximum length: 31	



---

Parameter	Description	Type	Size	Default
modem2-extension	FortiExtender interface name.	string	Maximum length: 31	

## file-filter

This section includes syntax for the following commands:

- [config file-filter profile on page 158](#)

### config file-filter profile

Configure file-filter profiles.

```
config file-filter profile
  Description: Configure file-filter profiles.
  edit <name>
    set comment {var-string}
    set extended-log [disable|enable]
    set feature-set [flow|proxy]
    set log [disable|enable]
    set replacemsg-group {string}
    config rules
      Description: File filter rules.
      edit <name>
        set comment {var-string}
        set protocol {option1}, {option2}, ...
        set action [log-only|block]
        set direction [incoming|outgoing|...]
        set password-protected [yes|any]
        set file-type <name1>, <name2>, ...
      next
    end
    set scan-archive-contents [disable|enable]
  next
end
```

### config file-filter profile

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 255	
extended-log	Enable/disable file-filter extended logging.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable extended logging.		
	<i>enable</i>	Enable extended logging.		
feature-set	Flow/proxy feature set.	option	-	flow

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>flow</i>	Flow feature set.		
	<i>proxy</i>	Proxy feature set.		
log	Enable/disable file-filter logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable logging.		
	<i>enable</i>	Enable logging.		
name	Profile name.	string	Maximum length: 35	
replacemsg-group	Replacement message group.	string	Maximum length: 35	
scan-archive-contents	Enable/disable archive contents scan.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable scanning archive contents.		
	<i>enable</i>	Enable scanning archive contents.		

## config rules

Parameter	Description	Type	Size	Default
name	File-filter rule name.	string	Maximum length: 35	
comment	Comment.	var-string	Maximum length: 255	
protocol	Protocols to apply rule to.	option	-	http ftp smtp imap pop3 mapi cifs ssh
	<b>Option</b>	<b>Description</b>		
	<i>http</i>	Filter on HTTP.		
	<i>ftp</i>	Filter on FTP.		
	<i>smtp</i>	Filter on SMTP.		

Parameter	Description	Type	Size	Default												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>imap</i></td><td>Filter on IMAP.</td></tr><tr><td><i>pop3</i></td><td>Filter on POP3.</td></tr><tr><td><i>mapi</i></td><td>Filter on MAPI. (Proxy mode only.)</td></tr><tr><td><i>cifs</i></td><td>Filter on CIFS.</td></tr><tr><td><i>ssh</i></td><td>Filter on SFTP and SCP. (Proxy mode only.)</td></tr></table>	Option	Description	<i>imap</i>	Filter on IMAP.	<i>pop3</i>	Filter on POP3.	<i>mapi</i>	Filter on MAPI. (Proxy mode only.)	<i>cifs</i>	Filter on CIFS.	<i>ssh</i>	Filter on SFTP and SCP. (Proxy mode only.)			
	Option	Description														
	<i>imap</i>	Filter on IMAP.														
	<i>pop3</i>	Filter on POP3.														
	<i>mapi</i>	Filter on MAPI. (Proxy mode only.)														
	<i>cifs</i>	Filter on CIFS.														
<i>ssh</i>	Filter on SFTP and SCP. (Proxy mode only.)															
action	Action taken for matched file.	option	-	log-only												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>log-only</i></td><td>Allow the content and write a log message.</td></tr><tr><td><i>block</i></td><td>Block the content and write a log message.</td></tr></table>	Option	Description	<i>log-only</i>	Allow the content and write a log message.	<i>block</i>	Block the content and write a log message.									
	Option	Description														
	<i>log-only</i>	Allow the content and write a log message.														
<i>block</i>	Block the content and write a log message.															
direction	Traffic direction (HTTP, FTP, SSH, CIFS only).	option	-	any												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>incoming</i></td><td>Match files transmitted in the session's reply direction.</td></tr><tr><td><i>outgoing</i></td><td>Match files transmitted in the session's originating direction.</td></tr><tr><td><i>any</i></td><td>Match files transmitted in the session's originating and reply directions.</td></tr></table>	Option	Description	<i>incoming</i>	Match files transmitted in the session's reply direction.	<i>outgoing</i>	Match files transmitted in the session's originating direction.	<i>any</i>	Match files transmitted in the session's originating and reply directions.							
	Option	Description														
	<i>incoming</i>	Match files transmitted in the session's reply direction.														
	<i>outgoing</i>	Match files transmitted in the session's originating direction.														
<i>any</i>	Match files transmitted in the session's originating and reply directions.															
password-protected	Match password-protected files.	option	-	any												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>yes</i></td><td>Match only password-protected files.</td></tr><tr><td><i>any</i></td><td>Match any file.</td></tr></table>	Option	Description	<i>yes</i>	Match only password-protected files.	<i>any</i>	Match any file.									
	Option	Description														
	<i>yes</i>	Match only password-protected files.														
<i>any</i>	Match any file.															
file-type <name>	Select file type. File type name.	string	Maximum length: 39													

# firewall

This section includes syntax for the following commands:

- [config firewall DoS-policy on page 163](#)
- [config firewall DoS-policy6 on page 165](#)
- [config firewall access-proxy-ssh-client-cert on page 168](#)
- [config firewall access-proxy-virtual-host on page 170](#)
- [config firewall access-proxy on page 171](#)
- [config firewall access-proxy6 on page 192](#)
- [config firewall acl on page 213](#)
- [config firewall acl6 on page 214](#)
- [config firewall address on page 215](#)
- [config firewall address6-template on page 221](#)
- [config firewall address6 on page 222](#)
- [config firewall addrgrp on page 226](#)
- [config firewall addrgrp6 on page 228](#)
- [config firewall auth-portal on page 229](#)
- [config firewall central-snat-map on page 230](#)
- [config firewall city on page 232](#)
- [config firewall country on page 233](#)
- [config firewall decrypted-traffic-mirror on page 233](#)
- [config firewall dnstranslation on page 234](#)
- [config firewall gtp on page 236](#)
- [config firewall identity-based-route on page 269](#)
- [config firewall interface-policy on page 270](#)
- [config firewall interface-policy6 on page 273](#)
- [config firewall internet-service-addition on page 276](#)
- [config firewall internet-service-append on page 277](#)
- [config firewall internet-service-botnet on page 278](#)
- [config firewall internet-service-custom-group on page 278](#)
- [config firewall internet-service-custom on page 279](#)
- [config firewall internet-service-definition on page 280](#)
- [config firewall internet-service-extension on page 282](#)
- [config firewall internet-service-group on page 285](#)
- [config firewall internet-service-ipbl-reason on page 286](#)
- [config firewall internet-service-ipbl-vendor on page 286](#)
- [config firewall internet-service-list on page 287](#)
- [config firewall internet-service-name on page 287](#)
- [config firewall internet-service-owner on page 288](#)
- [config firewall internet-service-reputation on page 289](#)

- 
- [config firewall internet-service-sld on page 289](#)
  - [config firewall internet-service on page 290](#)
  - [config firewall ip-translation on page 292](#)
  - [config firewall ipmacbinding setting on page 292](#)
  - [config firewall ipmacbinding table on page 293](#)
  - [config firewall ippool on page 294](#)
  - [config firewall ippool6 on page 298](#)
  - [config firewall ippool\\_grp on page 300](#)
  - [config firewall ipv6-eh-filter on page 301](#)
  - [config firewall ldb-monitor on page 302](#)
  - [config firewall local-in-policy on page 304](#)
  - [config firewall local-in-policy6 on page 306](#)
  - [config firewall multicast-address on page 308](#)
  - [config firewall multicast-address6 on page 310](#)
  - [config firewall multicast-policy on page 311](#)
  - [config firewall multicast-policy6 on page 313](#)
  - [config firewall pfcp on page 315](#)
  - [config firewall policy on page 318](#)
  - [config firewall profile-group on page 338](#)
  - [config firewall profile-protocol-options on page 340](#)
  - [config firewall proxy-address on page 364](#)
  - [config firewall proxy-addrgroup on page 368](#)
  - [config firewall proxy-policy on page 369](#)
  - [config firewall region on page 377](#)
  - [config firewall schedule group on page 377](#)
  - [config firewall schedule onetime on page 378](#)
  - [config firewall schedule recurring on page 379](#)
  - [config firewall security-policy on page 380](#)
  - [config firewall service category on page 388](#)
  - [config firewall service custom on page 388](#)
  - [config firewall service group on page 393](#)
  - [config firewall shaper per-ip-shaper on page 394](#)
  - [config firewall shaper traffic-shaper on page 395](#)
  - [config firewall shaping-policy on page 398](#)
  - [config firewall shaping-profile on page 402](#)
  - [config firewall sniffer on page 405](#)
  - [config firewall ssh host-key on page 410](#)
  - [config firewall ssh local-ca on page 412](#)
  - [config firewall ssh local-key on page 413](#)
  - [config firewall ssh setting on page 414](#)
  - [config firewall ssl-server on page 415](#)
  - [config firewall ssl-ssh-profile on page 417](#)
  - [config firewall ssl setting on page 446](#)

- [config firewall traffic-class on page 448](#)
- [config firewall ttl-policy on page 448](#)
- [config firewall vendor-mac on page 449](#)
- [config firewall vip on page 450](#)
- [config firewall vip6 on page 481](#)
- [config firewall vipgrp on page 510](#)
- [config firewall vipgrp6 on page 511](#)
- [config firewall wildcard-fqdn custom on page 512](#)
- [config firewall wildcard-fqdn group on page 513](#)

## config firewall DoS-policy

Configure IPv4 DoS policies.

```
config firewall DoS-policy
  Description: Configure IPv4 DoS policies.
  edit <policyid>
    config anomaly
      Description: Anomaly name.
      edit <name>
        set status [disable|enable]
        set log [enable|disable]
        set action [pass|block]
        set quarantine [none|attacker]
        set quarantine-expiry {user}
        set quarantine-log [disable|enable]
        set threshold {integer}
        set threshold(default) {integer}
      next
    end
    set comments {var-string}
    set dstaddr <name1>, <name2>, ...
    set interface {string}
    set name {string}
    set service <name1>, <name2>, ...
    set srcaddr <name1>, <name2>, ...
    set status [enable|disable]
  next
end
```

## config firewall DoS-policy

Parameter	Description	Type	Size	Default
comments	Comment.	var-string	Maximum length: 1023	
dstaddr <name>	Destination address name from available addresses. Address name.	string	Maximum length: 79	

Parameter	Description	Type	Size	Default						
interface	Incoming interface name from available interfaces.	string	Maximum length: 35							
name	Policy name.	string	Maximum length: 35							
policyid	Policy ID.	integer	Minimum value: 0 Maximum value: 9999 **	0						
service <name>	Service object from available options. Service name.	string	Maximum length: 79							
srcaddr <name>	Source address name from available addresses. Address name.	string	Maximum length: 79							
status	Enable/disable this policy.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable this policy.</td></tr><tr><td>disable</td><td>Disable this policy.</td></tr></table>				Option	Description	enable	Enable this policy.	disable	Disable this policy.
Option	Description									
enable	Enable this policy.									
disable	Disable this policy.									

\*\* Values may differ between models.

### config anomaly

Parameter	Description	Type	Size	Default
name	Anomaly name.	string	Maximum length: 63	
status	Enable/disable this anomaly.	option	-	disable
	<div><div>Option</div><div>Description</div></div>			
	<i>disable</i>	Disable this status.		
	<i>enable</i>	Enable this status.		
log	Enable/disable anomaly logging.	option	-	disable
	<div><div>Option</div><div>Description</div></div>			
	<i>enable</i>	Enable anomaly logging.		
	<i>disable</i>	Disable anomaly logging.		
action	Action taken when the threshold is reached.	option	-	pass



Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>pass</i></td><td>Allow traffic but record a log message if logging is enabled.</td></tr><tr><td><i>block</i></td><td>Block traffic if this anomaly is found.</td></tr></table>	Option	Description	<i>pass</i>	Allow traffic but record a log message if logging is enabled.	<i>block</i>	Block traffic if this anomaly is found.			
	Option	Description								
	<i>pass</i>	Allow traffic but record a log message if logging is enabled.								
<i>block</i>	Block traffic if this anomaly is found.									
quarantine	Quarantine method.	option	-	none						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>Quarantine is disabled.</td></tr><tr><td><i>attacker</i></td><td>Block all traffic sent from attacker's IP address. The attacker's IP address is also added to the banned user list. The target's address is not affected.</td></tr></table>	Option	Description	<i>none</i>	Quarantine is disabled.	<i>attacker</i>	Block all traffic sent from attacker's IP address. The attacker's IP address is also added to the banned user list. The target's address is not affected.			
	Option	Description								
	<i>none</i>	Quarantine is disabled.								
<i>attacker</i>	Block all traffic sent from attacker's IP address. The attacker's IP address is also added to the banned user list. The target's address is not affected.									
quarantine-expiry	Duration of quarantine.. Requires quarantine set to attacker.	user	Not Specified	5m						
quarantine-log	Enable/disable quarantine logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable quarantine logging.</td></tr><tr><td><i>enable</i></td><td>Enable quarantine logging.</td></tr></table>	Option	Description	<i>disable</i>	Disable quarantine logging.	<i>enable</i>	Enable quarantine logging.			
	Option	Description								
	<i>disable</i>	Disable quarantine logging.								
<i>enable</i>	Enable quarantine logging.									
threshold	Anomaly threshold. Number of detected instances (packets per second or concurrent session number) that triggers the anomaly action.	integer	Minimum value: 1 Maximum value: 2147483647	0						
threshold (default)	Number of detected instances. Note that each anomaly has a different threshold value assigned to it.	integer	Minimum value: 0 Maximum value: 4294967295	0						

## config firewall DoS-policy6

Configure IPv6 DoS policies.

```
config firewall DoS-policy6
  Description: Configure IPv6 DoS policies.
  edit <policyid>
    config anomaly
      Description: Anomaly name.
      edit <name>
        set status [disable|enable]
        set log [enable|disable]
        set action [pass|block]
```

```

        set quarantine [none|attacker]
        set quarantine-expiry {user}
        set quarantine-log [disable|enable]
        set threshold {integer}
        set threshold(default) {integer}
    next
end
set comments {var-string}
set dstaddr <name1>, <name2>, ...
set interface {string}
set name {string}
set service <name1>, <name2>, ...
set srcaddr <name1>, <name2>, ...
set status [enable|disable]
next
end

```

## config firewall DoS-policy6

Parameter	Description	Type	Size	Default
comments	Comment.	var-string	Maximum length: 1023	
dstaddr <name>	Destination address name from available addresses. Address name.	string	Maximum length: 79	
interface	Incoming interface name from available interfaces.	string	Maximum length: 35	
name	Policy name.	string	Maximum length: 35	
policyid	Policy ID.	integer	Minimum value: 0 Maximum value: 9999 **	0
service <name>	Service object from available options. Service name.	string	Maximum length: 79	
srcaddr <name>	Source address name from available addresses. Address name.	string	Maximum length: 79	
status	Enable/disable this policy.	option	-	enable
	Option	Description		
	enable	Enable this policy.		
	disable	Disable this policy.		

\*\* Values may differ between models.

## config anomaly

Parameter	Description	Type	Size	Default
name	Anomaly name.	string	Maximum length: 63	
status	Enable/disable this anomaly.	option	-	disable
	Option	Description		
	disable	Disable this status.		
	enable	Enable this status.		
log	Enable/disable anomaly logging.	option	-	disable
	Option	Description		
	enable	Enable anomaly logging.		
	disable	Disable anomaly logging.		
action	Action taken when the threshold is reached.	option	-	pass
	Option	Description		
	pass	Allow traffic but record a log message if logging is enabled.		
	block	Block traffic if this anomaly is found.		
quarantine	Quarantine method.	option	-	none
	Option	Description		
	none	Quarantine is disabled.		
	attacker	Block all traffic sent from attacker's IP address. The attacker's IP address is also added to the banned user list. The target's address is not affected.		
quarantine-expiry	Duration of quarantine.. Requires quarantine set to attacker.	user	Not Specified	5m
quarantine-log	Enable/disable quarantine logging.	option	-	enable
	Option	Description		
	disable	Disable quarantine logging.		
	enable	Enable quarantine logging.		

Parameter	Description	Type	Size	Default
threshold	Anomaly threshold. Number of detected instances (packets per second or concurrent session number) that triggers the anomaly action.	integer	Minimum value: 1 Maximum value: 2147483647	0
threshold (default)	Number of detected instances. Note that each anomaly has a different threshold value assigned to it.	integer	Minimum value: 0 Maximum value: 4294967295	0

## config firewall access-proxy-ssh-client-cert

Configure Access Proxy SSH client certificate.

```
config firewall access-proxy-ssh-client-cert
    Description: Configure Access Proxy SSH client certificate.
    edit <name>
        set auth-ca {string}
        config cert-extension
            Description: Configure certificate extension for user certificate.
            edit <name>
                set critical [no|yes]
                set type [fixed|user]
                set data {string}
            next
        end
        set permit-agent-forwarding [enable|disable]
        set permit-port-forwarding [enable|disable]
        set permit-pty [enable|disable]
        set permit-user-rc [enable|disable]
        set permit-x11-forwarding [enable|disable]
        set source-address [enable|disable]
    next
end
```

## config firewall access-proxy-ssh-client-cert

Parameter	Description	Type	Size	Default
auth-ca	Name of the SSH server public key authentication CA.	string	Maximum length: 79	
name	SSH client certificate name.	string	Maximum length: 79	
permit-agent-forwarding	Enable/disable appending permit-agent-forwarding certificate extension.	option	-	enable

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
permit-port-forwarding	Enable/disable appending permit-port-forwarding certificate extension.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
permit-pty	Enable/disable appending permit-pty certificate extension.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
permit-user-rc	Enable/disable appending permit-user-rc certificate extension.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
permit-x11-forwarding	Enable/disable appending permit-x11-forwarding certificate extension.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
source-address	Enable/disable appending source-address certificate critical option. This option ensure certificate only accepted from FortiGate source address.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

## config cert-extension

Parameter	Description	Type	Size	Default
name	Name of certificate extension.	string	Maximum length: 127	
critical	Critical option.	option	-	no
	<b>Option</b>	<b>Description</b>		
	<i>no</i>	Certificate extension, server ignores the unsupported certificate extension.		
	<i>yes</i>	Critical option, server refuses to authorize if it cannot recognize the critical option.		
type	Type of certificate extension.	option	-	fixed
	<b>Option</b>	<b>Description</b>		
	<i>fixed</i>	Fixed certificate extension entry.		
	<i>user</i>	Certificate extension entry filled with authenticated username.		
data	Data of certificate extension.	string	Maximum length: 127	

## config firewall access-proxy-virtual-host

Configure Access Proxy virtual hosts.

```
config firewall access-proxy-virtual-host
  Description: Configure Access Proxy virtual hosts.
  edit <name>
    set host {string}
    set host-type [sub-string|wildcard]
    set replacemsg-group {string}
    set ssl-certificate {string}
  next
end
```

## config firewall access-proxy-virtual-host

Parameter	Description	Type	Size	Default
host	The host name.	string	Maximum length: 79	
host-type	Type of host pattern.	option	-	sub-string

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>sub-string</i>	Match the pattern if a string contains the sub-string.		
	<i>wildcard</i>	Match the pattern with wildcards.		
name	Virtual host name.	string	Maximum length: 79	
replacemsg-group	Access-proxy-virtual-host replacement message override group.	string	Maximum length: 35	
ssl-certificate	SSL certificate for this host.	string	Maximum length: 35	

## config firewall access-proxy

Configure IPv4 access proxy.

```
config firewall access-proxy
    Description: Configure IPv4 access proxy.
    edit <name>
        config api-gateway
            Description: Set IPv4 API Gateway.
            edit <id>
                set url-map {string}
                set service [http|https|...]
                set ldb-method [static|round-robin|...]
                set virtual-host {string}
                set url-map-type [sub-string|wildcard|...]
            config realservers
                Description: Select the real servers that this Access Proxy will
                distribute traffic to.
                edit <id>
                    set addr-type [ip|fqdn]
                    set address {string}
                    set ip {ipv4-address-any}
                    set domain {string}
                    set port {integer}
                    set mappedport {user}
                    set status [active|standby|...]
                    set type [tcp-forwarding|ssh]
                    set weight {integer}
                    set http-host {string}
                    set health-check [disable|enable]
                    set health-check-proto [ping|http|...]
                    set holddown-interval [enable|disable]
                    set ssh-client-cert {string}
                    set ssh-host-key-validation [disable|enable]
                    set ssh-host-key <name1>, <name2>, ...
                next
            end
        set persistence [none|http-cookie]
```

```

set http-cookie-domain-from-host [disable|enable]
set http-cookie-domain {string}
set http-cookie-path {string}
set http-cookie-generation {integer}
set http-cookie-age {integer}
set http-cookie-share [disable|same-ip]
set https-cookie-secure [disable|enable]
set saml-server {string}
set saml-redirect [disable|enable]
set ssl-dh-bits [768|1024|...]
set ssl-algorithm [high|medium|...]
config ssl-cipher-suites
    Description: SSL/TLS cipher suites to offer to a server, ordered by
priority.
    edit <priority>
        set cipher [TLS-AES-128-GCM-SHA256|TLS-AES-256-GCM-SHA384|...]
        set versions {option1}, {option2}, ...
    next
end
set ssl-min-version [tls-1.0|tls-1.1|...]
set ssl-max-version [tls-1.0|tls-1.1|...]
set ssl-vpn-web-portal {string}
next
end
config api-gateway6
    Description: Set IPv6 API Gateway.
    edit <id>
        set url-map {string}
        set service [http|https|...]
        set ldb-method [static|round-robin|...]
        set virtual-host {string}
        set url-map-type [sub-string|wildcard|...]
        config realservers
            Description: Select the real servers that this Access Proxy will
distribute traffic to.
            edit <id>
                set addr-type [ip|fqdn]
                set address {string}
                set ip {ipv6-address}
                set domain {string}
                set port {integer}
                set mappedport {user}
                set status [active|standby|...]
                set type [tcp-forwarding|ssh]
                set weight {integer}
                set http-host {string}
                set health-check [disable|enable]
                set health-check-proto [ping|http|...]
                set holddown-interval [enable|disable]
                set ssh-client-cert {string}
                set ssh-host-key-validation [disable|enable]
                set ssh-host-key <name1>, <name2>, ...
            next
        end
        set persistence [none|http-cookie]
        set http-cookie-domain-from-host [disable|enable]

```



```

set http-cookie-domain {string}
set http-cookie-path {string}
set http-cookie-generation {integer}
set http-cookie-age {integer}
set http-cookie-share [disable|same-ip]
set https-cookie-secure [disable|enable]
set saml-server {string}
set saml-redirect [disable|enable]
set ssl-dh-bits [768|1024|...]
set ssl-algorithm [high|medium|...]
config ssl-cipher-suites
    Description: SSL/TLS cipher suites to offer to a server, ordered by
priority.
    edit <priority>
        set cipher [TLS-AES-128-GCM-SHA256|TLS-AES-256-GCM-SHA384|...]
        set versions {option1}, {option2}, ...
    next
end
set ssl-min-version [tls-1.0|tls-1.1|...]
set ssl-max-version [tls-1.0|tls-1.1|...]
set ssl-vpn-web-portal {string}
next
end
set auth-portal [disable|enable]
set auth-virtual-host {string}
set client-cert [disable|enable]
set decrypted-traffic-mirror {string}
set empty-cert-action [accept|block]
set log-blocked-traffic [enable|disable]
set vip {string}
next
end

```

## config firewall access-proxy

Parameter	Description	Type	Size	Default						
auth-portal	Enable/disable authentication portal.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable authentication portal.</td></tr><tr><td><i>enable</i></td><td>Enable authentication portal.</td></tr></table>				Option	Description	<i>disable</i>	Disable authentication portal.	<i>enable</i>	Enable authentication portal.
	Option	Description								
	<i>disable</i>	Disable authentication portal.								
	<i>enable</i>	Enable authentication portal.								
auth-virtual-host	Virtual host for authentication portal.	string	Maximum length: 79							
client-cert	Enable/disable to request client certificate.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable client certificate request.</td></tr><tr><td><i>enable</i></td><td>Enable client certificate request.</td></tr></table>				Option	Description	<i>disable</i>	Disable client certificate request.	<i>enable</i>	Enable client certificate request.
	Option	Description								
	<i>disable</i>	Disable client certificate request.								
	<i>enable</i>	Enable client certificate request.								

Parameter	Description	Type	Size	Default						
decrypted-traffic-mirror	Decrypted traffic mirror.	string	Maximum length: 35							
empty-cert-action	Action of an empty client certificate.	option	-	block						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>accept</i></td><td>Accept the SSL handshake if the client certificate is empty.</td></tr><tr><td><i>block</i></td><td>Block the SSL handshake if the client certificate is empty.</td></tr></table>				Option	Description	<i>accept</i>	Accept the SSL handshake if the client certificate is empty.	<i>block</i>	Block the SSL handshake if the client certificate is empty.
	Option	Description								
	<i>accept</i>	Accept the SSL handshake if the client certificate is empty.								
<i>block</i>	Block the SSL handshake if the client certificate is empty.									
log-blocked-traffic	Enable/disable logging of blocked traffic.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Log all traffic denied by this access proxy.</td></tr><tr><td><i>disable</i></td><td>Do not log all traffic denied by this access proxy.</td></tr></table>				Option	Description	<i>enable</i>	Log all traffic denied by this access proxy.	<i>disable</i>	Do not log all traffic denied by this access proxy.
	Option	Description								
	<i>enable</i>	Log all traffic denied by this access proxy.								
<i>disable</i>	Do not log all traffic denied by this access proxy.									
name	Access Proxy name.	string	Maximum length: 79							
vip	Virtual IP name.	string	Maximum length: 79							

### config api-gateway

Parameter	Description	Type	Size	Default												
id	API Gateway ID.	integer	Minimum value: 0 Maximum value: 4294967295	0												
url-map	URL pattern to match.	string	Maximum length: 511	/												
service	Service.	option	-	https												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>http</td><td>HTTP</td></tr><tr><td>https</td><td>HTTPS</td></tr><tr><td>tcp-forwarding</td><td>TCP-FORWARDING</td></tr><tr><td>samlsp</td><td>SAML-SP</td></tr><tr><td>web-portal</td><td>VPN-SSL-WEB-PORTAL</td></tr></table>				Option	Description	http	HTTP	https	HTTPS	tcp-forwarding	TCP-FORWARDING	samlsp	SAML-SP	web-portal	VPN-SSL-WEB-PORTAL
Option	Description															
http	HTTP															
https	HTTPS															
tcp-forwarding	TCP-FORWARDING															
samlsp	SAML-SP															
web-portal	VPN-SSL-WEB-PORTAL															

Parameter	Description	Type	Size	Default												
ldb-method	Method used to distribute sessions to real servers.	option	-	static												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>static</i></td><td>Distribute to server based on source IP.</td></tr><tr><td><i>round-robin</i></td><td>Distribute to server based round robin order.</td></tr><tr><td><i>weighted</i></td><td>Distribute to server based on weight.</td></tr><tr><td><i>first-alive</i></td><td>Distribute to the first server that is alive.</td></tr><tr><td><i>http-host</i></td><td>Distribute to server based on host field in HTTP header.</td></tr></table>	Option	Description	<i>static</i>	Distribute to server based on source IP.	<i>round-robin</i>	Distribute to server based round robin order.	<i>weighted</i>	Distribute to server based on weight.	<i>first-alive</i>	Distribute to the first server that is alive.	<i>http-host</i>	Distribute to server based on host field in HTTP header.			
	Option	Description														
	<i>static</i>	Distribute to server based on source IP.														
	<i>round-robin</i>	Distribute to server based round robin order.														
	<i>weighted</i>	Distribute to server based on weight.														
	<i>first-alive</i>	Distribute to the first server that is alive.														
<i>http-host</i>	Distribute to server based on host field in HTTP header.															
virtual-host	Virtual host.	string	Maximum length: 79													
url-map-type	Type of url-map.	option	-	sub-string												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>sub-string</i></td><td>Match the pattern if a string contains the sub-string.</td></tr><tr><td><i>wildcard</i></td><td>Match the pattern with wildcards.</td></tr><tr><td><i>regex</i></td><td>Match the pattern with a regular expression.</td></tr></table>	Option	Description	<i>sub-string</i>	Match the pattern if a string contains the sub-string.	<i>wildcard</i>	Match the pattern with wildcards.	<i>regex</i>	Match the pattern with a regular expression.							
	Option	Description														
	<i>sub-string</i>	Match the pattern if a string contains the sub-string.														
	<i>wildcard</i>	Match the pattern with wildcards.														
<i>regex</i>	Match the pattern with a regular expression.															
persistence	Configure how to make sure that clients connect to the same server every time they make a request that is part of the same session.	option	-	none												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>None.</td></tr><tr><td><i>http-cookie</i></td><td>HTTP cookie.</td></tr></table>	Option	Description	<i>none</i>	None.	<i>http-cookie</i>	HTTP cookie.									
	Option	Description														
	<i>none</i>	None.														
<i>http-cookie</i>	HTTP cookie.															
http-cookie-domain-from-host	Enable/disable use of HTTP cookie domain from host field in HTTP.	option	-	disable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable use of HTTP cookie domain from host field in HTTP (use http-cooke-domain setting).</td></tr><tr><td><i>enable</i></td><td>Enable use of HTTP cookie domain from host field in HTTP.</td></tr></table>	Option	Description	<i>disable</i>	Disable use of HTTP cookie domain from host field in HTTP (use http-cooke-domain setting).	<i>enable</i>	Enable use of HTTP cookie domain from host field in HTTP.									
	Option	Description														
	<i>disable</i>	Disable use of HTTP cookie domain from host field in HTTP (use http-cooke-domain setting).														
<i>enable</i>	Enable use of HTTP cookie domain from host field in HTTP.															
http-cookie-domain	Domain that HTTP cookie persistence should apply to.	string	Maximum length: 35													
http-cookie-path	Limit HTTP cookie persistence to the specified path.	string	Maximum length: 35													

Parameter	Description	Type	Size	Default
http-cookie-generation	Generation of HTTP cookie to be accepted. Changing invalidates all existing cookies.	integer	Minimum value: 0 Maximum value: 4294967295	0
http-cookie-age	Time in minutes that client web browsers should keep a cookie. Default is 60 minutes. 0 = no time limit.	integer	Minimum value: 0 Maximum value: 525600	60
http-cookie-share	Control sharing of cookies across API Gateway. Use of same-ip means a cookie from one virtual server can be used by another. Disable stops cookie sharing.	option	-	same-ip
	<b>Option</b>		<b>Description</b>	
	<i>disable</i>		Only allow HTTP cookie to match this API Gateway.	
	<i>same-ip</i>		Allow HTTP cookie to match any API Gateway with same IP.	
https-cookie-secure	Enable/disable verification that inserted HTTPS cookies are secure.	option	-	disable
	<b>Option</b>		<b>Description</b>	
	<i>disable</i>		Do not mark cookie as secure, allow sharing between an HTTP and HTTPS connection.	
	<i>enable</i>		Mark inserted cookie as secure, cookie can only be used for HTTPS a connection.	
saml-server	SAML service provider configuration for VIP authentication.	string	Maximum length: 35	
saml-redirect	Enable/disable SAML redirection after successful authentication.	option	-	disable
	<b>Option</b>		<b>Description</b>	
	<i>disable</i>		Do not support redirection after successful SAML authentication.	
	<i>enable</i>		Support redirection after successful SAML authentication.	
ssl-dh-bits	Number of bits to use in the Diffie-Hellman exchange for RSA encryption of SSL sessions.	option	-	2048
	<b>Option</b>		<b>Description</b>	
	768		768-bit Diffie-Hellman prime.	

Parameter	Description	Type	Size	Default												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>1024</td><td>1024-bit Diffie-Hellman prime.</td></tr><tr><td>1536</td><td>1536-bit Diffie-Hellman prime.</td></tr><tr><td>2048</td><td>2048-bit Diffie-Hellman prime.</td></tr><tr><td>3072</td><td>3072-bit Diffie-Hellman prime.</td></tr><tr><td>4096</td><td>4096-bit Diffie-Hellman prime.</td></tr></table>	Option	Description	1024	1024-bit Diffie-Hellman prime.	1536	1536-bit Diffie-Hellman prime.	2048	2048-bit Diffie-Hellman prime.	3072	3072-bit Diffie-Hellman prime.	4096	4096-bit Diffie-Hellman prime.			
	Option	Description														
	1024	1024-bit Diffie-Hellman prime.														
	1536	1536-bit Diffie-Hellman prime.														
	2048	2048-bit Diffie-Hellman prime.														
	3072	3072-bit Diffie-Hellman prime.														
	4096	4096-bit Diffie-Hellman prime.														
ssl-algorithm	Permitted encryption algorithms for the server side of SSL full mode sessions according to encryption strength.	option	-	high												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>high</td><td>High encryption. Allow only AES and ChaCha.</td></tr><tr><td>medium</td><td>Medium encryption. Allow AES, ChaCha, 3DES, and RC4.</td></tr><tr><td>low</td><td>Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.</td></tr></table>	Option	Description	high	High encryption. Allow only AES and ChaCha.	medium	Medium encryption. Allow AES, ChaCha, 3DES, and RC4.	low	Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.							
	Option	Description														
	high	High encryption. Allow only AES and ChaCha.														
	medium	Medium encryption. Allow AES, ChaCha, 3DES, and RC4.														
	low	Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.														
ssl-min-version	Lowest SSL/TLS version acceptable from a server.	option	-	tls-1.1												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>tls-1.0</td><td>TLS 1.0.</td></tr><tr><td>tls-1.1</td><td>TLS 1.1.</td></tr><tr><td>tls-1.2</td><td>TLS 1.2.</td></tr><tr><td>tls-1.3</td><td>TLS 1.3.</td></tr></table>	Option	Description	tls-1.0	TLS 1.0.	tls-1.1	TLS 1.1.	tls-1.2	TLS 1.2.	tls-1.3	TLS 1.3.					
	Option	Description														
	tls-1.0	TLS 1.0.														
	tls-1.1	TLS 1.1.														
	tls-1.2	TLS 1.2.														
	tls-1.3	TLS 1.3.														
ssl-max-version	Highest SSL/TLS version acceptable from a server.	option	-	tls-1.3												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>tls-1.0</td><td>TLS 1.0.</td></tr><tr><td>tls-1.1</td><td>TLS 1.1.</td></tr><tr><td>tls-1.2</td><td>TLS 1.2.</td></tr><tr><td>tls-1.3</td><td>TLS 1.3.</td></tr></table>	Option	Description	tls-1.0	TLS 1.0.	tls-1.1	TLS 1.1.	tls-1.2	TLS 1.2.	tls-1.3	TLS 1.3.					
	Option	Description														
	tls-1.0	TLS 1.0.														
	tls-1.1	TLS 1.1.														
	tls-1.2	TLS 1.2.														
	tls-1.3	TLS 1.3.														
ssl-vpn-web-portal	SSL-VPN web portal.	string	Maximum length: 35													

## config realservers

Parameter	Description	Type	Size	Default								
id	Real server ID.	integer	Minimum value: 0 Maximum value: 4294967295	0								
addr-type	Type of address.	option	-	ip								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ip</i></td><td>Standard IPv4 address.</td></tr><tr><td><i>fqdn</i></td><td>Non-wildcard FQDN address object.</td></tr></table>				Option	Description	<i>ip</i>	Standard IPv4 address.	<i>fqdn</i>	Non-wildcard FQDN address object.		
	Option	Description										
	<i>ip</i>	Standard IPv4 address.										
<i>fqdn</i>	Non-wildcard FQDN address object.											
address	Address or address group of the real server.	string	Maximum length: 79									
ip	IPv6 address of the real server.	ipv6-address	Not Specified	::								
domain	Wildcard domain name of the real server.	string	Maximum length: 255									
port	Port for communicating with the real server.	integer	Minimum value: 1 Maximum value: 65535	443								
mappedport	Port for communicating with the real server.	user	Not Specified									
status	Set the status of the real server to active so that it can accept traffic, or on standby or disabled so no traffic is sent.	option	-	active								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>active</i></td><td>Server status active.</td></tr><tr><td><i>standby</i></td><td>Server status standby.</td></tr><tr><td><i>disable</i></td><td>Server status disable.</td></tr></table>				Option	Description	<i>active</i>	Server status active.	<i>standby</i>	Server status standby.	<i>disable</i>	Server status disable.
	Option	Description										
	<i>active</i>	Server status active.										
	<i>standby</i>	Server status standby.										
<i>disable</i>	Server status disable.											
type	TCP forwarding server type.	option	-	tcp-forwarding								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>tcp-forwarding</i></td><td>TCP forwarding.</td></tr><tr><td><i>ssh</i></td><td>SSH.</td></tr></table>				Option	Description	<i>tcp-forwarding</i>	TCP forwarding.	<i>ssh</i>	SSH.		
	Option	Description										
	<i>tcp-forwarding</i>	TCP forwarding.										
<i>ssh</i>	SSH.											

Parameter	Description	Type	Size	Default								
weight	Weight of the real server. If weighted load balancing is enabled, the server with the highest weight gets more connections.	integer	Minimum value: 1 Maximum value: 255	1								
http-host	HTTP server domain name in HTTP header.	string	Maximum length: 63									
health-check	Enable to check the responsiveness of the real server before forwarding traffic.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable per server health check.</td></tr><tr><td>enable</td><td>Enable per server health check.</td></tr></table>	Option	Description	disable	Disable per server health check.	enable	Enable per server health check.					
Option	Description											
disable	Disable per server health check.											
enable	Enable per server health check.											
health-check-proto	Protocol of the health check monitor to use when polling to determine server's connectivity status.	option	-	ping								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ping</td><td>Use PING to test the link with the server.</td></tr><tr><td>http</td><td>Use HTTP-GET to test the link with the server.</td></tr><tr><td>tcp-connect</td><td>Use a full TCP connection to test the link with the server.</td></tr></table>	Option	Description	ping	Use PING to test the link with the server.	http	Use HTTP-GET to test the link with the server.	tcp-connect	Use a full TCP connection to test the link with the server.			
Option	Description											
ping	Use PING to test the link with the server.											
http	Use HTTP-GET to test the link with the server.											
tcp-connect	Use a full TCP connection to test the link with the server.											
holddown-interval	Enable/disable holddown timer. Server will be considered active and reachable once the holddown period has expired (30 seconds).	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable per server holddown.</td></tr><tr><td>disable</td><td>Disable per server holddown.</td></tr></table>	Option	Description	enable	Enable per server holddown.	disable	Disable per server holddown.					
Option	Description											
enable	Enable per server holddown.											
disable	Disable per server holddown.											
ssh-client-cert	Set access-proxy SSH client certificate profile.	string	Maximum length: 79									
ssh-host-key-validation	Enable/disable SSH real server host key validation.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable SSH real server host key validation.</td></tr><tr><td>enable</td><td>Enable SSH real server host key validation.</td></tr></table>	Option	Description	disable	Disable SSH real server host key validation.	enable	Enable SSH real server host key validation.					
Option	Description											
disable	Disable SSH real server host key validation.											
enable	Enable SSH real server host key validation.											
ssh-host-key<name>	One or more server host key. Server host key name.	string	Maximum length: 79									

## config ssl-cipher-suites

Parameter	Description	Type	Size	Default
priority	SSL/TLS cipher suites priority.	integer	Minimum value: 0 Maximum value: 4294967295	0
cipher	Cipher suite name.	option	-	

Option	Description
<i>TLS-AES-128-GCM-SHA256</i>	Cipher suite TLS-AES-128-GCM-SHA256.
<i>TLS-AES-256-GCM-SHA384</i>	Cipher suite TLS-AES-256-GCM-SHA384.
<i>TLS-CHACHA20-POLY1305-SHA256</i>	Cipher suite TLS-CHACHA20-POLY1305-SHA256.
<i>TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256</i>	Cipher suite TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256.
<i>TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256.
<i>TLS-DHE-RSA-WITH-CHACHA20-POLY1305-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-CHACHA20-POLY1305-SHA256.
<i>TLS-DHE-RSA-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA.
<i>TLS-DHE-RSA-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA.



Parameter	Description	Type	Size	Default																										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>TLS-DHE-RSA-WITH-AES-128-CBC-SHA256</i></td><td>Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA256.</td></tr><tr><td><i>TLS-DHE-RSA-WITH-AES-128-GCM-SHA256</i></td><td>Cipher suite TLS-DHE-RSA-WITH-AES-128-GCM-SHA256.</td></tr><tr><td><i>TLS-DHE-RSA-WITH-AES-256-CBC-SHA256</i></td><td>Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA256.</td></tr><tr><td><i>TLS-DHE-RSA-WITH-AES-256-GCM-SHA384</i></td><td>Cipher suite TLS-DHE-RSA-WITH-AES-256-GCM-SHA384.</td></tr><tr><td><i>TLS-DHE-DSS-WITH-AES-128-CBC-SHA</i></td><td>Cipher suite TLS-DHE-DSS-WITH-AES-128-CBC-SHA.</td></tr><tr><td><i>TLS-DHE-DSS-WITH-AES-256-CBC-SHA</i></td><td>Cipher suite TLS-DHE-DSS-WITH-AES-256-CBC-SHA.</td></tr><tr><td><i>TLS-DHE-DSS-WITH-AES-128-CBC-SHA256</i></td><td>Cipher suite TLS-DHE-DSS-WITH-AES-128-CBC-SHA256.</td></tr><tr><td><i>TLS-DHE-DSS-WITH-AES-128-GCM-SHA256</i></td><td>Cipher suite TLS-DHE-DSS-WITH-AES-128-GCM-SHA256.</td></tr><tr><td><i>TLS-DHE-DSS-WITH-AES-256-CBC-SHA256</i></td><td>Cipher suite TLS-DHE-DSS-WITH-AES-256-CBC-SHA256.</td></tr><tr><td><i>TLS-DHE-DSS-WITH-AES-256-GCM-SHA384</i></td><td>Cipher suite TLS-DHE-DSS-WITH-AES-256-GCM-SHA384.</td></tr><tr><td><i>TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA</i></td><td>Cipher suite TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA.</td></tr><tr><td><i>TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA256</i></td><td>Cipher suite TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA256.</td></tr></table>	Option	Description	<i>TLS-DHE-RSA-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA256.	<i>TLS-DHE-RSA-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-AES-128-GCM-SHA256.	<i>TLS-DHE-RSA-WITH-AES-256-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA256.	<i>TLS-DHE-RSA-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-DHE-RSA-WITH-AES-256-GCM-SHA384.	<i>TLS-DHE-DSS-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-AES-128-CBC-SHA.	<i>TLS-DHE-DSS-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-AES-256-CBC-SHA.	<i>TLS-DHE-DSS-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-AES-128-CBC-SHA256.	<i>TLS-DHE-DSS-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-AES-128-GCM-SHA256.	<i>TLS-DHE-DSS-WITH-AES-256-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-AES-256-CBC-SHA256.	<i>TLS-DHE-DSS-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-DHE-DSS-WITH-AES-256-GCM-SHA384.	<i>TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA.	<i>TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA256.			
Option	Description																													
<i>TLS-DHE-RSA-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA256.																													
<i>TLS-DHE-RSA-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-AES-128-GCM-SHA256.																													
<i>TLS-DHE-RSA-WITH-AES-256-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA256.																													
<i>TLS-DHE-RSA-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-DHE-RSA-WITH-AES-256-GCM-SHA384.																													
<i>TLS-DHE-DSS-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-AES-128-CBC-SHA.																													
<i>TLS-DHE-DSS-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-AES-256-CBC-SHA.																													
<i>TLS-DHE-DSS-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-AES-128-CBC-SHA256.																													
<i>TLS-DHE-DSS-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-AES-128-GCM-SHA256.																													
<i>TLS-DHE-DSS-WITH-AES-256-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-AES-256-CBC-SHA256.																													
<i>TLS-DHE-DSS-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-DHE-DSS-WITH-AES-256-GCM-SHA384.																													
<i>TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA.																													
<i>TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA256.																													

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>TLS-ECDHE-RSA-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-128-GCM-SHA256.		
	<i>TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA.		
	<i>TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA384.		
	<i>TLS-ECDHE-RSA-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-256-GCM-SHA384.		
	<i>TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA.		
	<i>TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA256.		
	<i>TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256.		
	<i>TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA.		
	<i>TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA384.		
	<i>TLS-ECDHE-ECDSA-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-256-GCM-SHA384.		

Parameter	Description	Type	Size	Default																										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>TLS-RSA-WITH-AES-128-CBC-SHA</i></td><td>Cipher suite TLS-RSA-WITH-AES-128-CBC-SHA.</td></tr><tr><td><i>TLS-RSA-WITH-AES-256-CBC-SHA</i></td><td>Cipher suite TLS-RSA-WITH-AES-256-CBC-SHA.</td></tr><tr><td><i>TLS-RSA-WITH-AES-128-CBC-SHA256</i></td><td>Cipher suite TLS-RSA-WITH-AES-128-CBC-SHA256.</td></tr><tr><td><i>TLS-RSA-WITH-AES-128-GCM-SHA256</i></td><td>Cipher suite TLS-RSA-WITH-AES-128-GCM-SHA256.</td></tr><tr><td><i>TLS-RSA-WITH-AES-256-CBC-SHA256</i></td><td>Cipher suite TLS-RSA-WITH-AES-256-CBC-SHA256.</td></tr><tr><td><i>TLS-RSA-WITH-AES-256-GCM-SHA384</i></td><td>Cipher suite TLS-RSA-WITH-AES-256-GCM-SHA384.</td></tr><tr><td><i>TLS-RSA-WITH-CAMELLIA-128-CBC-SHA</i></td><td>Cipher suite TLS-RSA-WITH-CAMELLIA-128-CBC-SHA.</td></tr><tr><td><i>TLS-RSA-WITH-CAMELLIA-256-CBC-SHA</i></td><td>Cipher suite TLS-RSA-WITH-CAMELLIA-256-CBC-SHA.</td></tr><tr><td><i>TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256</i></td><td>Cipher suite TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256.</td></tr><tr><td><i>TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256</i></td><td>Cipher suite TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256.</td></tr><tr><td><i>TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA</i></td><td>Cipher suite TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA.</td></tr><tr><td><i>TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA</i></td><td>Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA.</td></tr></table>	Option	Description	<i>TLS-RSA-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-AES-128-CBC-SHA.	<i>TLS-RSA-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-AES-256-CBC-SHA.	<i>TLS-RSA-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-AES-128-CBC-SHA256.	<i>TLS-RSA-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-RSA-WITH-AES-128-GCM-SHA256.	<i>TLS-RSA-WITH-AES-256-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-AES-256-CBC-SHA256.	<i>TLS-RSA-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-RSA-WITH-AES-256-GCM-SHA384.	<i>TLS-RSA-WITH-CAMELLIA-128-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-CAMELLIA-128-CBC-SHA.	<i>TLS-RSA-WITH-CAMELLIA-256-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-CAMELLIA-256-CBC-SHA.	<i>TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256.	<i>TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256.	<i>TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA.	<i>TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA.			
Option	Description																													
<i>TLS-RSA-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-AES-128-CBC-SHA.																													
<i>TLS-RSA-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-AES-256-CBC-SHA.																													
<i>TLS-RSA-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-AES-128-CBC-SHA256.																													
<i>TLS-RSA-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-RSA-WITH-AES-128-GCM-SHA256.																													
<i>TLS-RSA-WITH-AES-256-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-AES-256-CBC-SHA256.																													
<i>TLS-RSA-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-RSA-WITH-AES-256-GCM-SHA384.																													
<i>TLS-RSA-WITH-CAMELLIA-128-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-CAMELLIA-128-CBC-SHA.																													
<i>TLS-RSA-WITH-CAMELLIA-256-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-CAMELLIA-256-CBC-SHA.																													
<i>TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256.																													
<i>TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256.																													
<i>TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA.																													
<i>TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA.																													

Parameter	Description	Type	Size	Default																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA</td><td>Cipher suite TLS-DSS-RSA-WITH-CAMELLIA-128-CBC-SHA.</td></tr><tr><td>TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA</td><td>Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA.</td></tr><tr><td>TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA</td><td>Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA.</td></tr><tr><td>TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA256</td><td>Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA256.</td></tr><tr><td>TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256</td><td>Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256.</td></tr><tr><td>TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256</td><td>Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256.</td></tr><tr><td>TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256</td><td>Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256.</td></tr><tr><td>TLS-DHE-RSA-WITH-SEED-CBC-SHA</td><td>Cipher suite TLS-DHE-RSA-WITH-SEED-CBC-SHA.</td></tr><tr><td>TLS-DHE-DSS-WITH-SEED-CBC-SHA</td><td>Cipher suite TLS-DHE-DSS-WITH-SEED-CBC-SHA.</td></tr><tr><td>TLS-DHE-RSA-WITH-ARIA-128-CBC-SHA256</td><td>Cipher suite TLS-DHE-RSA-WITH-ARIA-128-CBC-SHA256.</td></tr></table>	Option	Description	TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA	Cipher suite TLS-DSS-RSA-WITH-CAMELLIA-128-CBC-SHA.	TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA.	TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA.	TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA256	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA256.	TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256.	TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256.	TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256.	TLS-DHE-RSA-WITH-SEED-CBC-SHA	Cipher suite TLS-DHE-RSA-WITH-SEED-CBC-SHA.	TLS-DHE-DSS-WITH-SEED-CBC-SHA	Cipher suite TLS-DHE-DSS-WITH-SEED-CBC-SHA.	TLS-DHE-RSA-WITH-ARIA-128-CBC-SHA256	Cipher suite TLS-DHE-RSA-WITH-ARIA-128-CBC-SHA256.			
Option	Description																									
TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA	Cipher suite TLS-DSS-RSA-WITH-CAMELLIA-128-CBC-SHA.																									
TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA.																									
TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA.																									
TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA256	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA256.																									
TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256.																									
TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256.																									
TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256.																									
TLS-DHE-RSA-WITH-SEED-CBC-SHA	Cipher suite TLS-DHE-RSA-WITH-SEED-CBC-SHA.																									
TLS-DHE-DSS-WITH-SEED-CBC-SHA	Cipher suite TLS-DHE-DSS-WITH-SEED-CBC-SHA.																									
TLS-DHE-RSA-WITH-ARIA-128-CBC-SHA256	Cipher suite TLS-DHE-RSA-WITH-ARIA-128-CBC-SHA256.																									

Parameter	Description	Type	Size	Default																								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>TLS-DHE-RSA-WITH-ARIA-256-CBC-SHA384</i></td><td>Cipher suite TLS-DHE-RSA-WITH-ARIA-256-CBC-SHA384.</td></tr><tr><td><i>TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256</i></td><td>Cipher suite TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256.</td></tr><tr><td><i>TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384</i></td><td>Cipher suite TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384.</td></tr><tr><td><i>TLS-RSA-WITH-SEED-CBC-SHA</i></td><td>Cipher suite TLS-RSA-WITH-SEED-CBC-SHA.</td></tr><tr><td><i>TLS-RSA-WITH-ARIA-128-CBC-SHA256</i></td><td>Cipher suite TLS-RSA-WITH-ARIA-128-CBC-SHA256.</td></tr><tr><td><i>TLS-RSA-WITH-ARIA-256-CBC-SHA384</i></td><td>Cipher suite TLS-RSA-WITH-ARIA-256-CBC-SHA384.</td></tr><tr><td><i>TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256</i></td><td>Cipher suite TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256.</td></tr><tr><td><i>TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384</i></td><td>Cipher suite TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384.</td></tr><tr><td><i>TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC-SHA256</i></td><td>Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC_SHA256.</td></tr><tr><td><i>TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC-SHA384</i></td><td>Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC_SHA384.</td></tr><tr><td><i>TLS-ECDHE-RSA-WITH-RC4-128-SHA</i></td><td>Cipher suite TLS-ECDHE-RSA-WITH-RC4-128-SHA.</td></tr></table>	Option	Description	<i>TLS-DHE-RSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-DHE-RSA-WITH-ARIA-256-CBC-SHA384.	<i>TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256.	<i>TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384.	<i>TLS-RSA-WITH-SEED-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-SEED-CBC-SHA.	<i>TLS-RSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-ARIA-128-CBC-SHA256.	<i>TLS-RSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-RSA-WITH-ARIA-256-CBC-SHA384.	<i>TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256.	<i>TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384.	<i>TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC_SHA256.	<i>TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC_SHA384.	<i>TLS-ECDHE-RSA-WITH-RC4-128-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-RC4-128-SHA.			
Option	Description																											
<i>TLS-DHE-RSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-DHE-RSA-WITH-ARIA-256-CBC-SHA384.																											
<i>TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256.																											
<i>TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384.																											
<i>TLS-RSA-WITH-SEED-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-SEED-CBC-SHA.																											
<i>TLS-RSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-ARIA-128-CBC-SHA256.																											
<i>TLS-RSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-RSA-WITH-ARIA-256-CBC-SHA384.																											
<i>TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256.																											
<i>TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384.																											
<i>TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC_SHA256.																											
<i>TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC_SHA384.																											
<i>TLS-ECDHE-RSA-WITH-RC4-128-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-RC4-128-SHA.																											

Parameter	Description	Type	Size	Default																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA</i></td><td>Cipher suite TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA.</td></tr><tr><td><i>TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA</i></td><td>Cipher suite TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA.</td></tr><tr><td><i>TLS-RSA-WITH-3DES-EDE-CBC-SHA</i></td><td>Cipher suite TLS-RSA-WITH-3DES-EDE-CBC-SHA.</td></tr><tr><td><i>TLS-RSA-WITH-RC4-128-MD5</i></td><td>Cipher suite TLS-RSA-WITH-RC4-128-MD5.</td></tr><tr><td><i>TLS-RSA-WITH-RC4-128-SHA</i></td><td>Cipher suite TLS-RSA-WITH-RC4-128-SHA.</td></tr><tr><td><i>TLS-DHE-RSA-WITH-DES-CBC-SHA</i></td><td>Cipher suite TLS-DHE-RSA-WITH-DES-CBC-SHA.</td></tr><tr><td><i>TLS-DHE-DSS-WITH-DES-CBC-SHA</i></td><td>Cipher suite TLS-DHE-DSS-WITH-DES-CBC-SHA.</td></tr><tr><td><i>TLS-RSA-WITH-DES-CBC-SHA</i></td><td>Cipher suite TLS-RSA-WITH-DES-CBC-SHA.</td></tr></table>	Option	Description	<i>TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA.	<i>TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA.	<i>TLS-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-3DES-EDE-CBC-SHA.	<i>TLS-RSA-WITH-RC4-128-MD5</i>	Cipher suite TLS-RSA-WITH-RC4-128-MD5.	<i>TLS-RSA-WITH-RC4-128-SHA</i>	Cipher suite TLS-RSA-WITH-RC4-128-SHA.	<i>TLS-DHE-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-DES-CBC-SHA.	<i>TLS-DHE-DSS-WITH-DES-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-DES-CBC-SHA.	<i>TLS-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-DES-CBC-SHA.			
	Option	Description																				
	<i>TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA.																				
	<i>TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA.																				
	<i>TLS-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-3DES-EDE-CBC-SHA.																				
	<i>TLS-RSA-WITH-RC4-128-MD5</i>	Cipher suite TLS-RSA-WITH-RC4-128-MD5.																				
	<i>TLS-RSA-WITH-RC4-128-SHA</i>	Cipher suite TLS-RSA-WITH-RC4-128-SHA.																				
	<i>TLS-DHE-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-DES-CBC-SHA.																				
	<i>TLS-DHE-DSS-WITH-DES-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-DES-CBC-SHA.																				
<i>TLS-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-DES-CBC-SHA.																					
versions	SSL/TLS versions that the cipher suite can be used with.	option	-	tls-1.0 tls-1.1 tls-1.2 tls-1.3																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>tls-1.0</i></td><td>TLS 1.0.</td></tr><tr><td><i>tls-1.1</i></td><td>TLS 1.1.</td></tr><tr><td><i>tls-1.2</i></td><td>TLS 1.2.</td></tr><tr><td><i>tls-1.3</i></td><td>TLS 1.3.</td></tr></table>	Option	Description	<i>tls-1.0</i>	TLS 1.0.	<i>tls-1.1</i>	TLS 1.1.	<i>tls-1.2</i>	TLS 1.2.	<i>tls-1.3</i>	TLS 1.3.											
	Option	Description																				
	<i>tls-1.0</i>	TLS 1.0.																				
	<i>tls-1.1</i>	TLS 1.1.																				
	<i>tls-1.2</i>	TLS 1.2.																				
<i>tls-1.3</i>	TLS 1.3.																					

## config api-gateway6

Parameter	Description	Type	Size	Default												
id	API Gateway ID.	integer	Minimum value: 0 Maximum value: 4294967295	0												
url-map	URL pattern to match.	string	Maximum length: 511	/												
service	Service.	option	-	https												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>http</td><td>HTTP</td></tr><tr><td>https</td><td>HTTPS</td></tr><tr><td>tcp-forwarding</td><td>TCP-FORWARDING</td></tr><tr><td>samlsp</td><td>SAML-SP</td></tr><tr><td>web-portal</td><td>VPN-SSL-WEB-PORTAL</td></tr></table>	Option	Description	http	HTTP	https	HTTPS	tcp-forwarding	TCP-FORWARDING	samlsp	SAML-SP	web-portal	VPN-SSL-WEB-PORTAL			
Option	Description															
http	HTTP															
https	HTTPS															
tcp-forwarding	TCP-FORWARDING															
samlsp	SAML-SP															
web-portal	VPN-SSL-WEB-PORTAL															
ldb-method	Method used to distribute sessions to real servers.	option	-	static												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>static</td><td>Distribute to server based on source IP.</td></tr><tr><td>round-robin</td><td>Distribute to server based round robin order.</td></tr><tr><td>weighted</td><td>Distribute to server based on weight.</td></tr><tr><td>first-alive</td><td>Distribute to the first server that is alive.</td></tr><tr><td>http-host</td><td>Distribute to server based on host field in HTTP header.</td></tr></table>	Option	Description	static	Distribute to server based on source IP.	round-robin	Distribute to server based round robin order.	weighted	Distribute to server based on weight.	first-alive	Distribute to the first server that is alive.	http-host	Distribute to server based on host field in HTTP header.			
Option	Description															
static	Distribute to server based on source IP.															
round-robin	Distribute to server based round robin order.															
weighted	Distribute to server based on weight.															
first-alive	Distribute to the first server that is alive.															
http-host	Distribute to server based on host field in HTTP header.															
virtual-host	Virtual host.	string	Maximum length: 79													
url-map-type	Type of url-map.	option	-	sub-string												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>sub-string</td><td>Match the pattern if a string contains the sub-string.</td></tr><tr><td>wildcard</td><td>Match the pattern with wildcards.</td></tr><tr><td>regex</td><td>Match the pattern with a regular expression.</td></tr></table>	Option	Description	sub-string	Match the pattern if a string contains the sub-string.	wildcard	Match the pattern with wildcards.	regex	Match the pattern with a regular expression.							
Option	Description															
sub-string	Match the pattern if a string contains the sub-string.															
wildcard	Match the pattern with wildcards.															
regex	Match the pattern with a regular expression.															
persistence	Configure how to make sure that clients connect to the same server every time they make a request that is part of the same session.	option	-	none												

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>None.</td></tr><tr><td><i>http-cookie</i></td><td>HTTP cookie.</td></tr></table>	Option	Description	<i>none</i>	None.	<i>http-cookie</i>	HTTP cookie.			
	Option	Description								
	<i>none</i>	None.								
<i>http-cookie</i>	HTTP cookie.									
http-cookie-domain-from-host	Enable/disable use of HTTP cookie domain from host field in HTTP.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable use of HTTP cookie domain from host field in HTTP (use http-cookies-domain setting).</td></tr><tr><td><i>enable</i></td><td>Enable use of HTTP cookie domain from host field in HTTP.</td></tr></table>	Option	Description	<i>disable</i>	Disable use of HTTP cookie domain from host field in HTTP (use http-cookies-domain setting).	<i>enable</i>	Enable use of HTTP cookie domain from host field in HTTP.			
	Option	Description								
	<i>disable</i>	Disable use of HTTP cookie domain from host field in HTTP (use http-cookies-domain setting).								
<i>enable</i>	Enable use of HTTP cookie domain from host field in HTTP.									
http-cookie-domain	Domain that HTTP cookie persistence should apply to.	string	Maximum length: 35							
http-cookie-path	Limit HTTP cookie persistence to the specified path.	string	Maximum length: 35							
http-cookie-generation	Generation of HTTP cookie to be accepted. Changing invalidates all existing cookies.	integer	Minimum value: 0 Maximum value: 4294967295	0						
http-cookie-age	Time in minutes that client web browsers should keep a cookie. Default is 60 minutes. 0 = no time limit.	integer	Minimum value: 0 Maximum value: 525600	60						
http-cookie-share	Control sharing of cookies across API Gateway. Use of same-ip means a cookie from one virtual server can be used by another. Disable stops cookie sharing.	option	-	same-ip						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Only allow HTTP cookie to match this API Gateway.</td></tr><tr><td><i>same-ip</i></td><td>Allow HTTP cookie to match any API Gateway with same IP.</td></tr></table>	Option	Description	<i>disable</i>	Only allow HTTP cookie to match this API Gateway.	<i>same-ip</i>	Allow HTTP cookie to match any API Gateway with same IP.			
	Option	Description								
	<i>disable</i>	Only allow HTTP cookie to match this API Gateway.								
<i>same-ip</i>	Allow HTTP cookie to match any API Gateway with same IP.									
https-cookie-secure	Enable/disable verification that inserted HTTPS cookies are secure.	option	-	disable						



Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Do not mark cookie as secure, allow sharing between an HTTP and HTTPS connection.		
	<i>enable</i>	Mark inserted cookie as secure, cookie can only be used for HTTPS a connection.		
saml-server	SAML service provider configuration for VIP authentication.	string	Maximum length: 35	
saml-redirect	Enable/disable SAML redirection after successful authentication.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Do not support redirection after successful SAML authentication.		
	<i>enable</i>	Support redirection after successful SAML authentication.		
ssl-dh-bits	Number of bits to use in the Diffie-Hellman exchange for RSA encryption of SSL sessions.	option	-	2048
	<b>Option</b>	<b>Description</b>		
	768	768-bit Diffie-Hellman prime.		
	1024	1024-bit Diffie-Hellman prime.		
	1536	1536-bit Diffie-Hellman prime.		
	2048	2048-bit Diffie-Hellman prime.		
	3072	3072-bit Diffie-Hellman prime.		
	4096	4096-bit Diffie-Hellman prime.		
ssl-algorithm	Permitted encryption algorithms for the server side of SSL full mode sessions according to encryption strength.	option	-	high
	<b>Option</b>	<b>Description</b>		
	high	High encryption. Allow only AES and ChaCha.		
	medium	Medium encryption. Allow AES, ChaCha, 3DES, and RC4.		
	low	Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.		
ssl-min-version	Lowest SSL/TLS version acceptable from a server.	option	-	tls-1.1

Parameter	Description	Type	Size	Default										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>tls-1.0</i></td><td>TLS 1.0.</td></tr><tr><td><i>tls-1.1</i></td><td>TLS 1.1.</td></tr><tr><td><i>tls-1.2</i></td><td>TLS 1.2.</td></tr><tr><td><i>tls-1.3</i></td><td>TLS 1.3.</td></tr></table>	Option	Description	<i>tls-1.0</i>	TLS 1.0.	<i>tls-1.1</i>	TLS 1.1.	<i>tls-1.2</i>	TLS 1.2.	<i>tls-1.3</i>	TLS 1.3.			
	Option	Description												
	<i>tls-1.0</i>	TLS 1.0.												
	<i>tls-1.1</i>	TLS 1.1.												
	<i>tls-1.2</i>	TLS 1.2.												
<i>tls-1.3</i>	TLS 1.3.													
ssl-max-version	Highest SSL/TLS version acceptable from a server.	option	-	tls-1.3										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>tls-1.0</i></td><td>TLS 1.0.</td></tr><tr><td><i>tls-1.1</i></td><td>TLS 1.1.</td></tr><tr><td><i>tls-1.2</i></td><td>TLS 1.2.</td></tr><tr><td><i>tls-1.3</i></td><td>TLS 1.3.</td></tr></table>	Option	Description	<i>tls-1.0</i>	TLS 1.0.	<i>tls-1.1</i>	TLS 1.1.	<i>tls-1.2</i>	TLS 1.2.	<i>tls-1.3</i>	TLS 1.3.			
	Option	Description												
	<i>tls-1.0</i>	TLS 1.0.												
	<i>tls-1.1</i>	TLS 1.1.												
	<i>tls-1.2</i>	TLS 1.2.												
<i>tls-1.3</i>	TLS 1.3.													
ssl-vpn-web-portal	SSL-VPN web portal.	string	Maximum length: 35											

### config realservers

Parameter	Description	Type	Size	Default
id	Real server ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
addr-type	Type of address.	option	-	ip
address	Address or address group of the real server.	string	Maximum length: 79	
ip	IPv6 address of the real server.	ipv6-address	Not Specified	::
domain	Wildcard domain name of the real server.	string	Maximum length: 255	
port	Port for communicating with the real server.	integer	Minimum value: 1 Maximum value: 65535	443
mappedport	Port for communicating with the real server.	user	Not Specified	

Parameter	Description	Type	Size	Default
status	Set the status of the real server to active so that it can accept traffic, or on standby or disabled so no traffic is sent.	option	-	active
type	TCP forwarding server type.	option	-	tcp-forwarding
weight	Weight of the real server. If weighted load balancing is enabled, the server with the highest weight gets more connections.	integer	Minimum value: 1 Maximum value: 255	1
http-host	HTTP server domain name in HTTP header.	string	Maximum length: 63	
health-check	Enable to check the responsiveness of the real server before forwarding traffic.	option	-	disable
health-check-proto	Protocol of the health check monitor to use when polling to determine server's connectivity status.	option	-	ping
holddown-interval	Enable/disable holddown timer. Server will be considered active and reachable once the holddown period has expired (30 seconds).	option	-	enable
ssh-client-cert	Set access-proxy SSH client certificate profile.	string	Maximum length: 79	
ssh-host-key-validation	Enable/disable SSH real server host key validation.	option	-	disable
ssh-host-key <name>	One or more server host key. Server host key name.	string	Maximum length: 79	

### config ssl-cipher-suites

Parameter	Description	Type	Size	Default
priority	SSL/TLS cipher suites priority.	integer	Minimum value: 0 Maximum value: 4294967295	0
cipher	Cipher suite name.	option	-	
versions	SSL/TLS versions that the cipher suite can be used with.	option	-	tls-1.0 tls-1.1 tls-1.2 tls-1.3

---

## config firewall access-proxy6

Configure IPv6 access proxy.

```
config firewall access-proxy6
    Description: Configure IPv6 access proxy.
    edit <name>
        config api-gateway
            Description: Set IPv4 API Gateway.
            edit <id>
                set url-map {string}
                set service [http|https|...]
                set ldb-method [static|round-robin|...]
                set virtual-host {string}
                set url-map-type [sub-string|wildcard|...]
            config realservers
                Description: Select the real servers that this Access Proxy will
                distribute traffic to.
                edit <id>
                    set addr-type [ip|fqdn]
                    set address {string}
                    set ip {ipv4-address-any}
                    set domain {string}
                    set port {integer}
                    set mappedport {user}
                    set status [active|standby|...]
                    set type [tcp-forwarding|ssh]
                    set weight {integer}
                    set http-host {string}
                    set health-check [disable|enable]
                    set health-check-proto [ping|http|...]
                    set holddown-interval [enable|disable]
                    set ssh-client-cert {string}
                    set ssh-host-key-validation [disable|enable]
                    set ssh-host-key <name1>, <name2>, ...
                next
            end
            set persistence [none|http-cookie]
            set http-cookie-domain-from-host [disable|enable]
            set http-cookie-domain {string}
            set http-cookie-path {string}
            set http-cookie-generation {integer}
            set http-cookie-age {integer}
            set http-cookie-share [disable|same-ip]
            set https-cookie-secure [disable|enable]
            set saml-server {string}
            set saml-redirect [disable|enable]
            set ssl-dh-bits [768|1024|...]
            set ssl-algorithm [high|medium|...]
            config ssl-cipher-suites
                Description: SSL/TLS cipher suites to offer to a server, ordered by
                priority.
                edit <priority>
                    set cipher [TLS-AES-128-GCM-SHA256|TLS-AES-256-GCM-SHA384|...]
                    set versions {option1}, {option2}, ...
                next
```

```

        end
        set ssl-min-version [tls-1.0|tls-1.1|...]
        set ssl-max-version [tls-1.0|tls-1.1|...]
        set ssl-vpn-web-portal {string}
    next
end
config api-gateway6
    Description: Set IPv6 API Gateway.
    edit <id>
        set url-map {string}
        set service [http|https|...]
        set ldb-method [static|round-robin|...]
        set virtual-host {string}
        set url-map-type [sub-string|wildcard|...]
        config realservers
            Description: Select the real servers that this Access Proxy will
distribute traffic to.
            edit <id>
                set addr-type [ip|fqdn]
                set address {string}
                set ip {ipv6-address}
                set domain {string}
                set port {integer}
                set mappedport {user}
                set status [active|standby|...]
                set type [tcp-forwarding|ssh]
                set weight {integer}
                set http-host {string}
                set health-check [disable|enable]
                set health-check-proto [ping|http|...]
                set holddown-interval [enable|disable]
                set ssh-client-cert {string}
                set ssh-host-key-validation [disable|enable]
                set ssh-host-key <name1>, <name2>, ...
            next
        end
        set persistence [none|http-cookie]
        set http-cookie-domain-from-host [disable|enable]
        set http-cookie-domain {string}
        set http-cookie-path {string}
        set http-cookie-generation {integer}
        set http-cookie-age {integer}
        set http-cookie-share [disable|same-ip]
        set https-cookie-secure [disable|enable]
        set saml-server {string}
        set saml-redirect [disable|enable]
        set ssl-dh-bits [768|1024|...]
        set ssl-algorithm [high|medium|...]
        config ssl-cipher-suites
            Description: SSL/TLS cipher suites to offer to a server, ordered by
priority.
            edit <priority>
                set cipher [TLS-AES-128-GCM-SHA256|TLS-AES-256-GCM-SHA384|...]
                set versions {option1}, {option2}, ...
            next
        end
    end
end

```

```

        set ssl-min-version [tls-1.0|tls-1.1|...]
        set ssl-max-version [tls-1.0|tls-1.1|...]
        set ssl-vpn-web-portal {string}
    next
end
set auth-portal [disable|enable]
set auth-virtual-host {string}
set client-cert [disable|enable]
set decrypted-traffic-mirror {string}
set empty-cert-action [accept|block]
set log-blocked-traffic [enable|disable]
set vip {string}
next
end

```

## config firewall access-proxy6

Parameter	Description	Type	Size	Default						
auth-portal	Enable/disable authentication portal.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable authentication portal.</td></tr><tr><td><i>enable</i></td><td>Enable authentication portal.</td></tr></table>	Option	Description	<i>disable</i>	Disable authentication portal.	<i>enable</i>	Enable authentication portal.			
Option	Description									
<i>disable</i>	Disable authentication portal.									
<i>enable</i>	Enable authentication portal.									
auth-virtual-host	Virtual host for authentication portal.	string	Maximum length: 79							
client-cert	Enable/disable to request client certificate.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable client certificate request.</td></tr><tr><td><i>enable</i></td><td>Enable client certificate request.</td></tr></table>	Option	Description	<i>disable</i>	Disable client certificate request.	<i>enable</i>	Enable client certificate request.			
Option	Description									
<i>disable</i>	Disable client certificate request.									
<i>enable</i>	Enable client certificate request.									
decrypted-traffic-mirror	Decrypted traffic mirror.	string	Maximum length: 35							
empty-cert-action	Action of an empty client certificate.	option	-	block						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>accept</i></td><td>Accept the SSL handshake if the client certificate is empty.</td></tr><tr><td><i>block</i></td><td>Block the SSL handshake if the client certificate is empty.</td></tr></table>	Option	Description	<i>accept</i>	Accept the SSL handshake if the client certificate is empty.	<i>block</i>	Block the SSL handshake if the client certificate is empty.			
Option	Description									
<i>accept</i>	Accept the SSL handshake if the client certificate is empty.									
<i>block</i>	Block the SSL handshake if the client certificate is empty.									
log-blocked-traffic	Enable/disable logging of blocked traffic.	option	-	disable						

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Log all traffic denied by this access proxy.		
	<i>disable</i>	Do not log all traffic denied by this access proxy.		
name	Access Proxy name.	string	Maximum length: 79	
vip	Virtual IP name.	string	Maximum length: 79	

### config api-gateway

Parameter	Description	Type	Size	Default
id	API Gateway ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
url-map	URL pattern to match.	string	Maximum length: 511	/
service	Service.	option	-	https
	<b>Option</b>	<b>Description</b>		
	<i>http</i>	HTTP		
	<i>https</i>	HTTPS		
	<i>tcp-forwarding</i>	TCP-FORWARDING		
	<i>samlsp</i>	SAML-SP		
	<i>web-portal</i>	VPN-SSL-WEB-PORTAL		
ldb-method	Method used to distribute sessions to real servers.	option	-	static
	<b>Option</b>	<b>Description</b>		
	<i>static</i>	Distribute to server based on source IP.		
	<i>round-robin</i>	Distribute to server based round robin order.		
	<i>weighted</i>	Distribute to server based on weight.		
	<i>first-alive</i>	Distribute to the first server that is alive.		
	<i>http-host</i>	Distribute to server based on host field in HTTP header.		
virtual-host	Virtual host.	string	Maximum length: 79	

Parameter	Description	Type	Size	Default								
url-map-type	Type of url-map.	option	-	sub-string								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>sub-string</td><td>Match the pattern if a string contains the sub-string.</td></tr><tr><td>wildcard</td><td>Match the pattern with wildcards.</td></tr><tr><td>regex</td><td>Match the pattern with a regular expression.</td></tr></table>				Option	Description	sub-string	Match the pattern if a string contains the sub-string.	wildcard	Match the pattern with wildcards.	regex	Match the pattern with a regular expression.
	Option	Description										
	sub-string	Match the pattern if a string contains the sub-string.										
	wildcard	Match the pattern with wildcards.										
regex	Match the pattern with a regular expression.											
persistence	Configure how to make sure that clients connect to the same server every time they make a request that is part of the same session.	option	-	none								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>none</td><td>None.</td></tr><tr><td>http-cookie</td><td>HTTP cookie.</td></tr></table>				Option	Description	none	None.	http-cookie	HTTP cookie.		
	Option	Description										
	none	None.										
http-cookie	HTTP cookie.											
http-cookie-domain-from-host	Enable/disable use of HTTP cookie domain from host field in HTTP.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable use of HTTP cookie domain from host field in HTTP (use http-cooke-domain setting).</td></tr><tr><td>enable</td><td>Enable use of HTTP cookie domain from host field in HTTP.</td></tr></table>				Option	Description	disable	Disable use of HTTP cookie domain from host field in HTTP (use http-cooke-domain setting).	enable	Enable use of HTTP cookie domain from host field in HTTP.		
	Option	Description										
	disable	Disable use of HTTP cookie domain from host field in HTTP (use http-cooke-domain setting).										
enable	Enable use of HTTP cookie domain from host field in HTTP.											
http-cookie-domain	Domain that HTTP cookie persistence should apply to.	string	Maximum length: 35									
http-cookie-path	Limit HTTP cookie persistence to the specified path.	string	Maximum length: 35									
http-cookie-generation	Generation of HTTP cookie to be accepted. Changing invalidates all existing cookies.	integer	Minimum value: 0 Maximum value: 4294967295	0								
http-cookie-age	Time in minutes that client web browsers should keep a cookie. Default is 60 minutes. 0 = no time limit.	integer	Minimum value: 0 Maximum value: 525600	60								
http-cookie-share	Control sharing of cookies across API Gateway. Use of same-ip means a cookie from one virtual server can be used by another. Disable stops cookie sharing.	option	-	same-ip								



Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Only allow HTTP cookie to match this API Gateway.		
	<i>same-ip</i>	Allow HTTP cookie to match any API Gateway with same IP.		
https-cookie-secure	Enable/disable verification that inserted HTTPS cookies are secure.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Do not mark cookie as secure, allow sharing between an HTTP and HTTPS connection.		
	<i>enable</i>	Mark inserted cookie as secure, cookie can only be used for HTTPS a connection.		
saml-server	SAML service provider configuration for VIP authentication.	string	Maximum length: 35	
saml-redirect	Enable/disable SAML redirection after successful authentication.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Do not support redirection after successful SAML authentication.		
	<i>enable</i>	Support redirection after successful SAML authentication.		
ssl-dh-bits	Number of bits to use in the Diffie-Hellman exchange for RSA encryption of SSL sessions.	option	-	2048
	<b>Option</b>	<b>Description</b>		
	768	768-bit Diffie-Hellman prime.		
	1024	1024-bit Diffie-Hellman prime.		
	1536	1536-bit Diffie-Hellman prime.		
	2048	2048-bit Diffie-Hellman prime.		
	3072	3072-bit Diffie-Hellman prime.		
	4096	4096-bit Diffie-Hellman prime.		
ssl-algorithm	Permitted encryption algorithms for the server side of SSL full mode sessions according to encryption strength.	option	-	high

Parameter	Description	Type	Size	Default										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>high</i></td><td>High encryption. Allow only AES and ChaCha.</td></tr><tr><td><i>medium</i></td><td>Medium encryption. Allow AES, ChaCha, 3DES, and RC4.</td></tr><tr><td><i>low</i></td><td>Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.</td></tr></table>	Option	Description	<i>high</i>	High encryption. Allow only AES and ChaCha.	<i>medium</i>	Medium encryption. Allow AES, ChaCha, 3DES, and RC4.	<i>low</i>	Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.					
	Option	Description												
	<i>high</i>	High encryption. Allow only AES and ChaCha.												
	<i>medium</i>	Medium encryption. Allow AES, ChaCha, 3DES, and RC4.												
<i>low</i>	Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.													
ssl-min-version	Lowest SSL/TLS version acceptable from a server.	option	-	tls-1.1										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>tls-1.0</i></td><td>TLS 1.0.</td></tr><tr><td><i>tls-1.1</i></td><td>TLS 1.1.</td></tr><tr><td><i>tls-1.2</i></td><td>TLS 1.2.</td></tr><tr><td><i>tls-1.3</i></td><td>TLS 1.3.</td></tr></table>	Option	Description	<i>tls-1.0</i>	TLS 1.0.	<i>tls-1.1</i>	TLS 1.1.	<i>tls-1.2</i>	TLS 1.2.	<i>tls-1.3</i>	TLS 1.3.			
	Option	Description												
	<i>tls-1.0</i>	TLS 1.0.												
	<i>tls-1.1</i>	TLS 1.1.												
	<i>tls-1.2</i>	TLS 1.2.												
<i>tls-1.3</i>	TLS 1.3.													
ssl-max-version	Highest SSL/TLS version acceptable from a server.	option	-	tls-1.3										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>tls-1.0</i></td><td>TLS 1.0.</td></tr><tr><td><i>tls-1.1</i></td><td>TLS 1.1.</td></tr><tr><td><i>tls-1.2</i></td><td>TLS 1.2.</td></tr><tr><td><i>tls-1.3</i></td><td>TLS 1.3.</td></tr></table>	Option	Description	<i>tls-1.0</i>	TLS 1.0.	<i>tls-1.1</i>	TLS 1.1.	<i>tls-1.2</i>	TLS 1.2.	<i>tls-1.3</i>	TLS 1.3.			
	Option	Description												
	<i>tls-1.0</i>	TLS 1.0.												
	<i>tls-1.1</i>	TLS 1.1.												
	<i>tls-1.2</i>	TLS 1.2.												
<i>tls-1.3</i>	TLS 1.3.													
ssl-vpn-web-portal	SSL-VPN web portal.	string	Maximum length: 35											

### config realservers

Parameter	Description	Type	Size	Default
id	Real server ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
addr-type	Type of address.	option	-	ip
	Option	Description		
	ip	Standard IPv4 address.		
	fqdn	Non-wildcard FQDN address object.		

Parameter	Description	Type	Size	Default								
address	Address or address group of the real server.	string	Maximum length: 79									
ip	IPv6 address of the real server.	ipv6-address	Not Specified	::								
domain	Wildcard domain name of the real server.	string	Maximum length: 255									
port	Port for communicating with the real server.	integer	Minimum value: 1 Maximum value: 65535	443								
mappedport	Port for communicating with the real server.	user	Not Specified									
status	Set the status of the real server to active so that it can accept traffic, or on standby or disabled so no traffic is sent.	option	-	active								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>active</td><td>Server status active.</td></tr><tr><td>standby</td><td>Server status standby.</td></tr><tr><td>disable</td><td>Server status disable.</td></tr></table>				Option	Description	active	Server status active.	standby	Server status standby.	disable	Server status disable.
Option	Description											
active	Server status active.											
standby	Server status standby.											
disable	Server status disable.											
type	TCP forwarding server type.	option	-	tcp-forwarding								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>tcp-forwarding</td><td>TCP forwarding.</td></tr><tr><td>ssh</td><td>SSH.</td></tr></table>				Option	Description	tcp-forwarding	TCP forwarding.	ssh	SSH.		
Option	Description											
tcp-forwarding	TCP forwarding.											
ssh	SSH.											
weight	Weight of the real server. If weighted load balancing is enabled, the server with the highest weight gets more connections.	integer	Minimum value: 1 Maximum value: 255	1								
http-host	HTTP server domain name in HTTP header.	string	Maximum length: 63									
health-check	Enable to check the responsiveness of the real server before forwarding traffic.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable per server health check.</td></tr><tr><td>enable</td><td>Enable per server health check.</td></tr></table>				Option	Description	disable	Disable per server health check.	enable	Enable per server health check.		
Option	Description											
disable	Disable per server health check.											
enable	Enable per server health check.											

Parameter	Description	Type	Size	Default								
health-check-proto	Protocol of the health check monitor to use when polling to determine server's connectivity status.	option	-	ping								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ping</i></td><td>Use PING to test the link with the server.</td></tr><tr><td><i>http</i></td><td>Use HTTP-GET to test the link with the server.</td></tr><tr><td><i>tcp-connect</i></td><td>Use a full TCP connection to test the link with the server.</td></tr></table>	Option	Description	<i>ping</i>	Use PING to test the link with the server.	<i>http</i>	Use HTTP-GET to test the link with the server.	<i>tcp-connect</i>	Use a full TCP connection to test the link with the server.			
Option	Description											
<i>ping</i>	Use PING to test the link with the server.											
<i>http</i>	Use HTTP-GET to test the link with the server.											
<i>tcp-connect</i>	Use a full TCP connection to test the link with the server.											
holddown-interval	Enable/disable holddown timer. Server will be considered active and reachable once the holddown period has expired (30 seconds).	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable per server holddown.</td></tr><tr><td><i>disable</i></td><td>Disable per server holddown.</td></tr></table>	Option	Description	<i>enable</i>	Enable per server holddown.	<i>disable</i>	Disable per server holddown.					
Option	Description											
<i>enable</i>	Enable per server holddown.											
<i>disable</i>	Disable per server holddown.											
ssh-client-cert	Set access-proxy SSH client certificate profile.	string	Maximum length: 79									
ssh-host-key-validation	Enable/disable SSH real server host key validation.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable SSH real server host key validation.</td></tr><tr><td><i>enable</i></td><td>Enable SSH real server host key validation.</td></tr></table>	Option	Description	<i>disable</i>	Disable SSH real server host key validation.	<i>enable</i>	Enable SSH real server host key validation.					
Option	Description											
<i>disable</i>	Disable SSH real server host key validation.											
<i>enable</i>	Enable SSH real server host key validation.											
ssh-host-key<name>	One or more server host key. Server host key name.	string	Maximum length: 79									

### config ssl-cipher-suites

Parameter	Description	Type	Size	Default
priority	SSL/TLS cipher suites priority.	integer	Minimum value: 0 Maximum value: 4294967295	0
cipher	Cipher suite name.	option	-	

Parameter	Description	Type	Size	Default																								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>TLS-AES-128-GCM-SHA256</td><td>Cipher suite TLS-AES-128-GCM-SHA256.</td></tr><tr><td>TLS-AES-256-GCM-SHA384</td><td>Cipher suite TLS-AES-256-GCM-SHA384.</td></tr><tr><td>TLS-CHACHA20-POLY1305-SHA256</td><td>Cipher suite TLS-CHACHA20-POLY1305-SHA256.</td></tr><tr><td>TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256</td><td>Cipher suite TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256.</td></tr><tr><td>TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256</td><td>Cipher suite TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256.</td></tr><tr><td>TLS-DHE-RSA-WITH-CHACHA20-POLY1305-SHA256</td><td>Cipher suite TLS-DHE-RSA-WITH-CHACHA20-POLY1305-SHA256.</td></tr><tr><td>TLS-DHE-RSA-WITH-AES-128-CBC-SHA</td><td>Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA.</td></tr><tr><td>TLS-DHE-RSA-WITH-AES-256-CBC-SHA</td><td>Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA.</td></tr><tr><td>TLS-DHE-RSA-WITH-AES-128-CBC-SHA256</td><td>Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA256.</td></tr><tr><td>TLS-DHE-RSA-WITH-AES-128-GCM-SHA256</td><td>Cipher suite TLS-DHE-RSA-WITH-AES-128-GCM-SHA256.</td></tr><tr><td>TLS-DHE-RSA-WITH-AES-256-CBC-SHA256</td><td>Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA256.</td></tr></table>	Option	Description	TLS-AES-128-GCM-SHA256	Cipher suite TLS-AES-128-GCM-SHA256.	TLS-AES-256-GCM-SHA384	Cipher suite TLS-AES-256-GCM-SHA384.	TLS-CHACHA20-POLY1305-SHA256	Cipher suite TLS-CHACHA20-POLY1305-SHA256.	TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256	Cipher suite TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256.	TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256	Cipher suite TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256.	TLS-DHE-RSA-WITH-CHACHA20-POLY1305-SHA256	Cipher suite TLS-DHE-RSA-WITH-CHACHA20-POLY1305-SHA256.	TLS-DHE-RSA-WITH-AES-128-CBC-SHA	Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA.	TLS-DHE-RSA-WITH-AES-256-CBC-SHA	Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA.	TLS-DHE-RSA-WITH-AES-128-CBC-SHA256	Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA256.	TLS-DHE-RSA-WITH-AES-128-GCM-SHA256	Cipher suite TLS-DHE-RSA-WITH-AES-128-GCM-SHA256.	TLS-DHE-RSA-WITH-AES-256-CBC-SHA256	Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA256.			
Option	Description																											
TLS-AES-128-GCM-SHA256	Cipher suite TLS-AES-128-GCM-SHA256.																											
TLS-AES-256-GCM-SHA384	Cipher suite TLS-AES-256-GCM-SHA384.																											
TLS-CHACHA20-POLY1305-SHA256	Cipher suite TLS-CHACHA20-POLY1305-SHA256.																											
TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256	Cipher suite TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256.																											
TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256	Cipher suite TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256.																											
TLS-DHE-RSA-WITH-CHACHA20-POLY1305-SHA256	Cipher suite TLS-DHE-RSA-WITH-CHACHA20-POLY1305-SHA256.																											
TLS-DHE-RSA-WITH-AES-128-CBC-SHA	Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA.																											
TLS-DHE-RSA-WITH-AES-256-CBC-SHA	Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA.																											
TLS-DHE-RSA-WITH-AES-128-CBC-SHA256	Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA256.																											
TLS-DHE-RSA-WITH-AES-128-GCM-SHA256	Cipher suite TLS-DHE-RSA-WITH-AES-128-GCM-SHA256.																											
TLS-DHE-RSA-WITH-AES-256-CBC-SHA256	Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA256.																											

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>TLS-DHE-RSA-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-DHE-RSA-WITH-AES-256-GCM-SHA384.		
	<i>TLS-DHE-DSS-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-AES-128-CBC-SHA.		
	<i>TLS-DHE-DSS-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-AES-256-CBC-SHA.		
	<i>TLS-DHE-DSS-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-AES-128-CBC-SHA256.		
	<i>TLS-DHE-DSS-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-AES-128-GCM-SHA256.		
	<i>TLS-DHE-DSS-WITH-AES-256-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-AES-256-CBC-SHA256.		
	<i>TLS-DHE-DSS-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-DHE-DSS-WITH-AES-256-GCM-SHA384.		
	<i>TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA.		
	<i>TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA256.		
	<i>TLS-ECDHE-RSA-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-128-GCM-SHA256.		
	<i>TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA.		

Parameter	Description	Type	Size	Default																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA384</i></td><td>Cipher suite TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA384.</td></tr><tr><td><i>TLS-ECDHE-RSA-WITH-AES-256-GCM-SHA384</i></td><td>Cipher suite TLS-ECDHE-RSA-WITH-AES-256-GCM-SHA384.</td></tr><tr><td><i>TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA</i></td><td>Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA.</td></tr><tr><td><i>TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA256</i></td><td>Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA256.</td></tr><tr><td><i>TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256</i></td><td>Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256.</td></tr><tr><td><i>TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA</i></td><td>Cipher suite TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA.</td></tr><tr><td><i>TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA384</i></td><td>Cipher suite TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA384.</td></tr><tr><td><i>TLS-ECDHE-ECDSA-WITH-AES-256-GCM-SHA384</i></td><td>Cipher suite TLS-ECDHE-ECDSA-WITH-AES-256-GCM-SHA384.</td></tr><tr><td><i>TLS-RSA-WITH-AES-128-CBC-SHA</i></td><td>Cipher suite TLS-RSA-WITH-AES-128-CBC-SHA.</td></tr><tr><td><i>TLS-RSA-WITH-AES-256-CBC-SHA</i></td><td>Cipher suite TLS-RSA-WITH-AES-256-CBC-SHA.</td></tr></table>	Option	Description	<i>TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA384.	<i>TLS-ECDHE-RSA-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-256-GCM-SHA384.	<i>TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA.	<i>TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA256.	<i>TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256.	<i>TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA.	<i>TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA384.	<i>TLS-ECDHE-ECDSA-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-256-GCM-SHA384.	<i>TLS-RSA-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-AES-128-CBC-SHA.	<i>TLS-RSA-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-AES-256-CBC-SHA.			
Option	Description																									
<i>TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA384.																									
<i>TLS-ECDHE-RSA-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-256-GCM-SHA384.																									
<i>TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA.																									
<i>TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA256.																									
<i>TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256.																									
<i>TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA.																									
<i>TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA384.																									
<i>TLS-ECDHE-ECDSA-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-256-GCM-SHA384.																									
<i>TLS-RSA-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-AES-128-CBC-SHA.																									
<i>TLS-RSA-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-AES-256-CBC-SHA.																									

Parameter	Description	Type	Size	Default																								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>TLS-RSA-WITH-AES-128-CBC-SHA256</td><td>Cipher suite TLS-RSA-WITH-AES-128-CBC-SHA256.</td></tr><tr><td>TLS-RSA-WITH-AES-128-GCM-SHA256</td><td>Cipher suite TLS-RSA-WITH-AES-128-GCM-SHA256.</td></tr><tr><td>TLS-RSA-WITH-AES-256-CBC-SHA256</td><td>Cipher suite TLS-RSA-WITH-AES-256-CBC-SHA256.</td></tr><tr><td>TLS-RSA-WITH-AES-256-GCM-SHA384</td><td>Cipher suite TLS-RSA-WITH-AES-256-GCM-SHA384.</td></tr><tr><td>TLS-RSA-WITH-CAMELLIA-128-CBC-SHA</td><td>Cipher suite TLS-RSA-WITH-CAMELLIA-128-CBC-SHA.</td></tr><tr><td>TLS-RSA-WITH-CAMELLIA-256-CBC-SHA</td><td>Cipher suite TLS-RSA-WITH-CAMELLIA-256-CBC-SHA.</td></tr><tr><td>TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256</td><td>Cipher suite TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256.</td></tr><tr><td>TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256</td><td>Cipher suite TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256.</td></tr><tr><td>TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA</td><td>Cipher suite TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA.</td></tr><tr><td>TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA</td><td>Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA.</td></tr><tr><td>TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA</td><td>Cipher suite TLS-DSS-RSA-WITH-CAMELLIA-128-CBC-SHA.</td></tr></table>	Option	Description	TLS-RSA-WITH-AES-128-CBC-SHA256	Cipher suite TLS-RSA-WITH-AES-128-CBC-SHA256.	TLS-RSA-WITH-AES-128-GCM-SHA256	Cipher suite TLS-RSA-WITH-AES-128-GCM-SHA256.	TLS-RSA-WITH-AES-256-CBC-SHA256	Cipher suite TLS-RSA-WITH-AES-256-CBC-SHA256.	TLS-RSA-WITH-AES-256-GCM-SHA384	Cipher suite TLS-RSA-WITH-AES-256-GCM-SHA384.	TLS-RSA-WITH-CAMELLIA-128-CBC-SHA	Cipher suite TLS-RSA-WITH-CAMELLIA-128-CBC-SHA.	TLS-RSA-WITH-CAMELLIA-256-CBC-SHA	Cipher suite TLS-RSA-WITH-CAMELLIA-256-CBC-SHA.	TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256	Cipher suite TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256.	TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256	Cipher suite TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256.	TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA	Cipher suite TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA.	TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA.	TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA	Cipher suite TLS-DSS-RSA-WITH-CAMELLIA-128-CBC-SHA.			
Option	Description																											
TLS-RSA-WITH-AES-128-CBC-SHA256	Cipher suite TLS-RSA-WITH-AES-128-CBC-SHA256.																											
TLS-RSA-WITH-AES-128-GCM-SHA256	Cipher suite TLS-RSA-WITH-AES-128-GCM-SHA256.																											
TLS-RSA-WITH-AES-256-CBC-SHA256	Cipher suite TLS-RSA-WITH-AES-256-CBC-SHA256.																											
TLS-RSA-WITH-AES-256-GCM-SHA384	Cipher suite TLS-RSA-WITH-AES-256-GCM-SHA384.																											
TLS-RSA-WITH-CAMELLIA-128-CBC-SHA	Cipher suite TLS-RSA-WITH-CAMELLIA-128-CBC-SHA.																											
TLS-RSA-WITH-CAMELLIA-256-CBC-SHA	Cipher suite TLS-RSA-WITH-CAMELLIA-256-CBC-SHA.																											
TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256	Cipher suite TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256.																											
TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256	Cipher suite TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256.																											
TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA	Cipher suite TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA.																											
TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA.																											
TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA	Cipher suite TLS-DSS-RSA-WITH-CAMELLIA-128-CBC-SHA.																											



Parameter	Description	Type	Size	Default																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA</i></td><td>Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA.</td></tr><tr><td><i>TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA</i></td><td>Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA.</td></tr><tr><td><i>TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA256</i></td><td>Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA256.</td></tr><tr><td><i>TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256</i></td><td>Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256.</td></tr><tr><td><i>TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256</i></td><td>Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256.</td></tr><tr><td><i>TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256</i></td><td>Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256.</td></tr><tr><td><i>TLS-DHE-RSA-WITH-SEED-CBC-SHA</i></td><td>Cipher suite TLS-DHE-RSA-WITH-SEED-CBC-SHA.</td></tr><tr><td><i>TLS-DHE-DSS-WITH-SEED-CBC-SHA</i></td><td>Cipher suite TLS-DHE-DSS-WITH-SEED-CBC-SHA.</td></tr><tr><td><i>TLS-DHE-RSA-WITH-ARIA-128-CBC-SHA256</i></td><td>Cipher suite TLS-DHE-RSA-WITH-ARIA-128-CBC-SHA256.</td></tr><tr><td><i>TLS-DHE-RSA-WITH-ARIA-256-CBC-SHA384</i></td><td>Cipher suite TLS-DHE-RSA-WITH-ARIA-256-CBC-SHA384.</td></tr></table>	Option	Description	<i>TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA.	<i>TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA.	<i>TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA256.	<i>TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256.	<i>TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256.	<i>TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256.	<i>TLS-DHE-RSA-WITH-SEED-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-SEED-CBC-SHA.	<i>TLS-DHE-DSS-WITH-SEED-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-SEED-CBC-SHA.	<i>TLS-DHE-RSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-ARIA-128-CBC-SHA256.	<i>TLS-DHE-RSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-DHE-RSA-WITH-ARIA-256-CBC-SHA384.			
Option	Description																									
<i>TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA.																									
<i>TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA.																									
<i>TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA256.																									
<i>TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256.																									
<i>TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256.																									
<i>TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256.																									
<i>TLS-DHE-RSA-WITH-SEED-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-SEED-CBC-SHA.																									
<i>TLS-DHE-DSS-WITH-SEED-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-SEED-CBC-SHA.																									
<i>TLS-DHE-RSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-ARIA-128-CBC-SHA256.																									
<i>TLS-DHE-RSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-DHE-RSA-WITH-ARIA-256-CBC-SHA384.																									

Parameter	Description	Type	Size	Default																								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256</i></td><td>Cipher suite TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256.</td></tr><tr><td><i>TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384</i></td><td>Cipher suite TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384.</td></tr><tr><td><i>TLS-RSA-WITH-SEED-CBC-SHA</i></td><td>Cipher suite TLS-RSA-WITH-SEED-CBC-SHA.</td></tr><tr><td><i>TLS-RSA-WITH-ARIA-128-CBC-SHA256</i></td><td>Cipher suite TLS-RSA-WITH-ARIA-128-CBC-SHA256.</td></tr><tr><td><i>TLS-RSA-WITH-ARIA-256-CBC-SHA384</i></td><td>Cipher suite TLS-RSA-WITH-ARIA-256-CBC-SHA384.</td></tr><tr><td><i>TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256</i></td><td>Cipher suite TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256.</td></tr><tr><td><i>TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384</i></td><td>Cipher suite TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384.</td></tr><tr><td><i>TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC-SHA256</i></td><td>Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC_SHA256.</td></tr><tr><td><i>TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC-SHA384</i></td><td>Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC_SHA384.</td></tr><tr><td><i>TLS-ECDHE-RSA-WITH-RC4-128-SHA</i></td><td>Cipher suite TLS-ECDHE-RSA-WITH-RC4-128-SHA.</td></tr><tr><td><i>TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA</i></td><td>Cipher suite TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA.</td></tr></table>	Option	Description	<i>TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256.	<i>TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384.	<i>TLS-RSA-WITH-SEED-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-SEED-CBC-SHA.	<i>TLS-RSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-ARIA-128-CBC-SHA256.	<i>TLS-RSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-RSA-WITH-ARIA-256-CBC-SHA384.	<i>TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256.	<i>TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384.	<i>TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC_SHA256.	<i>TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC_SHA384.	<i>TLS-ECDHE-RSA-WITH-RC4-128-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-RC4-128-SHA.	<i>TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA.			
Option	Description																											
<i>TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256.																											
<i>TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384.																											
<i>TLS-RSA-WITH-SEED-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-SEED-CBC-SHA.																											
<i>TLS-RSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-ARIA-128-CBC-SHA256.																											
<i>TLS-RSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-RSA-WITH-ARIA-256-CBC-SHA384.																											
<i>TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256.																											
<i>TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384.																											
<i>TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC_SHA256.																											
<i>TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC_SHA384.																											
<i>TLS-ECDHE-RSA-WITH-RC4-128-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-RC4-128-SHA.																											
<i>TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA.																											

Parameter	Description	Type	Size	Default																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA</i></td><td>Cipher suite TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA.</td></tr><tr><td><i>TLS-RSA-WITH-3DES-EDE-CBC-SHA</i></td><td>Cipher suite TLS-RSA-WITH-3DES-EDE-CBC-SHA.</td></tr><tr><td><i>TLS-RSA-WITH-RC4-128-MD5</i></td><td>Cipher suite TLS-RSA-WITH-RC4-128-MD5.</td></tr><tr><td><i>TLS-RSA-WITH-RC4-128-SHA</i></td><td>Cipher suite TLS-RSA-WITH-RC4-128-SHA.</td></tr><tr><td><i>TLS-DHE-RSA-WITH-DES-CBC-SHA</i></td><td>Cipher suite TLS-DHE-RSA-WITH-DES-CBC-SHA.</td></tr><tr><td><i>TLS-DHE-DSS-WITH-DES-CBC-SHA</i></td><td>Cipher suite TLS-DHE-DSS-WITH-DES-CBC-SHA.</td></tr><tr><td><i>TLS-RSA-WITH-DES-CBC-SHA</i></td><td>Cipher suite TLS-RSA-WITH-DES-CBC-SHA.</td></tr></table>	Option	Description	<i>TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA.	<i>TLS-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-3DES-EDE-CBC-SHA.	<i>TLS-RSA-WITH-RC4-128-MD5</i>	Cipher suite TLS-RSA-WITH-RC4-128-MD5.	<i>TLS-RSA-WITH-RC4-128-SHA</i>	Cipher suite TLS-RSA-WITH-RC4-128-SHA.	<i>TLS-DHE-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-DES-CBC-SHA.	<i>TLS-DHE-DSS-WITH-DES-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-DES-CBC-SHA.	<i>TLS-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-DES-CBC-SHA.			
	Option	Description																		
	<i>TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA.																		
	<i>TLS-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-3DES-EDE-CBC-SHA.																		
	<i>TLS-RSA-WITH-RC4-128-MD5</i>	Cipher suite TLS-RSA-WITH-RC4-128-MD5.																		
	<i>TLS-RSA-WITH-RC4-128-SHA</i>	Cipher suite TLS-RSA-WITH-RC4-128-SHA.																		
	<i>TLS-DHE-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-DES-CBC-SHA.																		
	<i>TLS-DHE-DSS-WITH-DES-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-DES-CBC-SHA.																		
<i>TLS-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-DES-CBC-SHA.																			
versions	SSL/TLS versions that the cipher suite can be used with.	option	-	tls-1.0 tls-1.1 tls-1.2 tls-1.3																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>tls-1.0</i></td><td>TLS 1.0.</td></tr><tr><td><i>tls-1.1</i></td><td>TLS 1.1.</td></tr><tr><td><i>tls-1.2</i></td><td>TLS 1.2.</td></tr><tr><td><i>tls-1.3</i></td><td>TLS 1.3.</td></tr></table>	Option	Description	<i>tls-1.0</i>	TLS 1.0.	<i>tls-1.1</i>	TLS 1.1.	<i>tls-1.2</i>	TLS 1.2.	<i>tls-1.3</i>	TLS 1.3.									
	Option	Description																		
	<i>tls-1.0</i>	TLS 1.0.																		
	<i>tls-1.1</i>	TLS 1.1.																		
	<i>tls-1.2</i>	TLS 1.2.																		
<i>tls-1.3</i>	TLS 1.3.																			

## config api-gateway6

Parameter	Description	Type	Size	Default
id	API Gateway ID.	integer	Minimum value: 0 Maximum value: 4294967295	0

Parameter	Description	Type	Size	Default												
url-map	URL pattern to match.	string	Maximum length: 511	/												
service	Service.	option	-	https												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>http</td><td>HTTP</td></tr><tr><td>https</td><td>HTTPS</td></tr><tr><td>tcp-forwarding</td><td>TCP-FORWARDING</td></tr><tr><td>samlsp</td><td>SAML-SP</td></tr><tr><td>web-portal</td><td>VPN-SSL-WEB-PORTAL</td></tr></table>	Option	Description	http	HTTP	https	HTTPS	tcp-forwarding	TCP-FORWARDING	samlsp	SAML-SP	web-portal	VPN-SSL-WEB-PORTAL			
Option	Description															
http	HTTP															
https	HTTPS															
tcp-forwarding	TCP-FORWARDING															
samlsp	SAML-SP															
web-portal	VPN-SSL-WEB-PORTAL															
ldb-method	Method used to distribute sessions to real servers.	option	-	static												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>static</td><td>Distribute to server based on source IP.</td></tr><tr><td>round-robin</td><td>Distribute to server based round robin order.</td></tr><tr><td>weighted</td><td>Distribute to server based on weight.</td></tr><tr><td>first-alive</td><td>Distribute to the first server that is alive.</td></tr><tr><td>http-host</td><td>Distribute to server based on host field in HTTP header.</td></tr></table>	Option	Description	static	Distribute to server based on source IP.	round-robin	Distribute to server based round robin order.	weighted	Distribute to server based on weight.	first-alive	Distribute to the first server that is alive.	http-host	Distribute to server based on host field in HTTP header.			
Option	Description															
static	Distribute to server based on source IP.															
round-robin	Distribute to server based round robin order.															
weighted	Distribute to server based on weight.															
first-alive	Distribute to the first server that is alive.															
http-host	Distribute to server based on host field in HTTP header.															
virtual-host	Virtual host.	string	Maximum length: 79													
url-map-type	Type of url-map.	option	-	sub-string												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>sub-string</td><td>Match the pattern if a string contains the sub-string.</td></tr><tr><td>wildcard</td><td>Match the pattern with wildcards.</td></tr><tr><td>regex</td><td>Match the pattern with a regular expression.</td></tr></table>	Option	Description	sub-string	Match the pattern if a string contains the sub-string.	wildcard	Match the pattern with wildcards.	regex	Match the pattern with a regular expression.							
Option	Description															
sub-string	Match the pattern if a string contains the sub-string.															
wildcard	Match the pattern with wildcards.															
regex	Match the pattern with a regular expression.															
persistence	Configure how to make sure that clients connect to the same server every time they make a request that is part of the same session.	option	-	none												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>none</td><td>None.</td></tr><tr><td>http-cookie</td><td>HTTP cookie.</td></tr></table>	Option	Description	none	None.	http-cookie	HTTP cookie.									
Option	Description															
none	None.															
http-cookie	HTTP cookie.															

Parameter	Description	Type	Size	Default
http-cookie-domain-from-host	Enable/disable use of HTTP cookie domain from host field in HTTP.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable use of HTTP cookie domain from host field in HTTP (use http-cookies-domain setting).		
	<i>enable</i>	Enable use of HTTP cookie domain from host field in HTTP.		
http-cookie-domain	Domain that HTTP cookie persistence should apply to.	string	Maximum length: 35	
http-cookie-path	Limit HTTP cookie persistence to the specified path.	string	Maximum length: 35	
http-cookie-generation	Generation of HTTP cookie to be accepted. Changing invalidates all existing cookies.	integer	Minimum value: 0 Maximum value: 4294967295	0
http-cookie-age	Time in minutes that client web browsers should keep a cookie. Default is 60 minutes. 0 = no time limit.	integer	Minimum value: 0 Maximum value: 525600	60
http-cookie-share	Control sharing of cookies across API Gateway. Use of same-ip means a cookie from one virtual server can be used by another. Disable stops cookie sharing.	option	-	same-ip
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Only allow HTTP cookie to match this API Gateway.		
	<i>same-ip</i>	Allow HTTP cookie to match any API Gateway with same IP.		
https-cookie-secure	Enable/disable verification that inserted HTTPS cookies are secure.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Do not mark cookie as secure, allow sharing between an HTTP and HTTPS connection.		
	<i>enable</i>	Mark inserted cookie as secure, cookie can only be used for HTTPS a connection.		
saml-server	SAML service provider configuration for VIP authentication.	string	Maximum length: 35	

Parameter	Description	Type	Size	Default														
saml-redirect	Enable/disable SAML redirection after successful authentication.	option	-	disable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Do not support redirection after successful SAML authentication.</td></tr><tr><td><i>enable</i></td><td>Support redirection after successful SAML authentication.</td></tr></table>	Option	Description	<i>disable</i>	Do not support redirection after successful SAML authentication.	<i>enable</i>	Support redirection after successful SAML authentication.											
Option	Description																	
<i>disable</i>	Do not support redirection after successful SAML authentication.																	
<i>enable</i>	Support redirection after successful SAML authentication.																	
ssl-dh-bits	Number of bits to use in the Diffie-Hellman exchange for RSA encryption of SSL sessions.	option	-	2048														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>768</i></td><td>768-bit Diffie-Hellman prime.</td></tr><tr><td><i>1024</i></td><td>1024-bit Diffie-Hellman prime.</td></tr><tr><td><i>1536</i></td><td>1536-bit Diffie-Hellman prime.</td></tr><tr><td><i>2048</i></td><td>2048-bit Diffie-Hellman prime.</td></tr><tr><td><i>3072</i></td><td>3072-bit Diffie-Hellman prime.</td></tr><tr><td><i>4096</i></td><td>4096-bit Diffie-Hellman prime.</td></tr></table>	Option	Description	<i>768</i>	768-bit Diffie-Hellman prime.	<i>1024</i>	1024-bit Diffie-Hellman prime.	<i>1536</i>	1536-bit Diffie-Hellman prime.	<i>2048</i>	2048-bit Diffie-Hellman prime.	<i>3072</i>	3072-bit Diffie-Hellman prime.	<i>4096</i>	4096-bit Diffie-Hellman prime.			
Option	Description																	
<i>768</i>	768-bit Diffie-Hellman prime.																	
<i>1024</i>	1024-bit Diffie-Hellman prime.																	
<i>1536</i>	1536-bit Diffie-Hellman prime.																	
<i>2048</i>	2048-bit Diffie-Hellman prime.																	
<i>3072</i>	3072-bit Diffie-Hellman prime.																	
<i>4096</i>	4096-bit Diffie-Hellman prime.																	
ssl-algorithm	Permitted encryption algorithms for the server side of SSL full mode sessions according to encryption strength.	option	-	high														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>high</i></td><td>High encryption. Allow only AES and ChaCha.</td></tr><tr><td><i>medium</i></td><td>Medium encryption. Allow AES, ChaCha, 3DES, and RC4.</td></tr><tr><td><i>low</i></td><td>Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.</td></tr></table>	Option	Description	<i>high</i>	High encryption. Allow only AES and ChaCha.	<i>medium</i>	Medium encryption. Allow AES, ChaCha, 3DES, and RC4.	<i>low</i>	Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.									
Option	Description																	
<i>high</i>	High encryption. Allow only AES and ChaCha.																	
<i>medium</i>	Medium encryption. Allow AES, ChaCha, 3DES, and RC4.																	
<i>low</i>	Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.																	
ssl-min-version	Lowest SSL/TLS version acceptable from a server.	option	-	tls-1.1														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>tls-1.0</i></td><td>TLS 1.0.</td></tr><tr><td><i>tls-1.1</i></td><td>TLS 1.1.</td></tr><tr><td><i>tls-1.2</i></td><td>TLS 1.2.</td></tr><tr><td><i>tls-1.3</i></td><td>TLS 1.3.</td></tr></table>	Option	Description	<i>tls-1.0</i>	TLS 1.0.	<i>tls-1.1</i>	TLS 1.1.	<i>tls-1.2</i>	TLS 1.2.	<i>tls-1.3</i>	TLS 1.3.							
Option	Description																	
<i>tls-1.0</i>	TLS 1.0.																	
<i>tls-1.1</i>	TLS 1.1.																	
<i>tls-1.2</i>	TLS 1.2.																	
<i>tls-1.3</i>	TLS 1.3.																	
ssl-max-version	Highest SSL/TLS version acceptable from a server.	option	-	tls-1.3														

Parameter	Description	Type	Size	Default										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>tls-1.0</i></td><td>TLS 1.0.</td></tr><tr><td><i>tls-1.1</i></td><td>TLS 1.1.</td></tr><tr><td><i>tls-1.2</i></td><td>TLS 1.2.</td></tr><tr><td><i>tls-1.3</i></td><td>TLS 1.3.</td></tr></table>	Option	Description	<i>tls-1.0</i>	TLS 1.0.	<i>tls-1.1</i>	TLS 1.1.	<i>tls-1.2</i>	TLS 1.2.	<i>tls-1.3</i>	TLS 1.3.			
	Option	Description												
	<i>tls-1.0</i>	TLS 1.0.												
	<i>tls-1.1</i>	TLS 1.1.												
	<i>tls-1.2</i>	TLS 1.2.												
<i>tls-1.3</i>	TLS 1.3.													
ssl-vpn-web-portal	SSL-VPN web portal.	string	Maximum length: 35											

### config realservers

Parameter	Description	Type	Size	Default
id	Real server ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
addr-type	Type of address.	option	-	ip
address	Address or address group of the real server.	string	Maximum length: 79	
ip	IPv6 address of the real server.	ipv6-address	Not Specified	::
domain	Wildcard domain name of the real server.	string	Maximum length: 255	
port	Port for communicating with the real server.	integer	Minimum value: 1 Maximum value: 65535	443
mappedport	Port for communicating with the real server.	user	Not Specified	
status	Set the status of the real server to active so that it can accept traffic, or on standby or disabled so no traffic is sent.	option	-	active
type	TCP forwarding server type.	option	-	tcp-forwarding
weight	Weight of the real server. If weighted load balancing is enabled, the server with the highest weight gets more connections.	integer	Minimum value: 1 Maximum value: 255	1

Parameter	Description	Type	Size	Default
http-host	HTTP server domain name in HTTP header.	string	Maximum length: 63	
health-check	Enable to check the responsiveness of the real server before forwarding traffic.	option	-	disable
health-check-proto	Protocol of the health check monitor to use when polling to determine server's connectivity status.	option	-	ping
holddown-interval	Enable/disable holddown timer. Server will be considered active and reachable once the holddown period has expired (30 seconds).	option	-	enable
ssh-client-cert	Set access-proxy SSH client certificate profile.	string	Maximum length: 79	
ssh-host-key-validation	Enable/disable SSH real server host key validation.	option	-	disable
ssh-host-key <name>	One or more server host key. Server host key name.	string	Maximum length: 79	

#### config ssl-cipher-suites

Parameter	Description	Type	Size	Default
priority	SSL/TLS cipher suites priority.	integer	Minimum value: 0 Maximum value: 4294967295	0
cipher	Cipher suite name.	option	-	
versions	SSL/TLS versions that the cipher suite can be used with.	option	-	tls-1.0 tls-1.1 tls-1.2 tls-1.3



## config firewall acl



This command is available for model(s): FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200F, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F.

It is not available for: FortiGate 1000D, FortiGate 200E, FortiGate 201E, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 5001E1, FortiGate 5001E, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

Configure IPv4 access control list.

```
config firewall acl
  Description: Configure IPv4 access control list.
  edit <policyid>
    set comments {var-string}
    set dstaddr <name1>, <name2>, ...
    set interface {string}
    set name {string}
    set service <name1>, <name2>, ...
    set srcaddr <name1>, <name2>, ...
    set status [enable|disable]
  next
end
```

## config firewall acl

Parameter	Description	Type	Size	Default
comments	Comment.	var-string	Maximum length: 1023	
dstaddr <name>	Destination address name. Address name.	string	Maximum length: 79	

Parameter	Description	Type	Size	Default						
interface	Interface name.	string	Maximum length: 35							
name	Policy name.	string	Maximum length: 35							
policyid	Policy ID.	integer	Minimum value: 0 Maximum value: 9999	0						
service <name>	Service name. Service name.	string	Maximum length: 79							
srcaddr <name>	Source address name. Address name.	string	Maximum length: 79							
status	Enable/disable access control list status.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable access control list status.</td></tr><tr><td>disable</td><td>Disable access control list status.</td></tr></table>				Option	Description	enable	Enable access control list status.	disable	Disable access control list status.
Option	Description									
enable	Enable access control list status.									
disable	Disable access control list status.									

## config firewall acl6



This command is available for model(s): FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200F, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F.

It is not available for: FortiGate 1000D, FortiGate 200E, FortiGate 201E, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 5001E1, FortiGate 5001E, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

Configure IPv6 access control list.

```
config firewall acl6
    Description: Configure IPv6 access control list.
    edit <policyid>
        set comments {var-string}
        set dstaddr <name1>, <name2>, ...
        set interface {string}
        set name {string}
        set service <name1>, <name2>, ...
        set srcaddr <name1>, <name2>, ...
        set status [enable|disable]
    next
end
```

## config firewall acl6

Parameter	Description	Type	Size	Default
comments	Comment.	var-string	Maximum length: 1023	
dstaddr <name>	Destination address name. Address name.	string	Maximum length: 79	
interface	Interface name.	string	Maximum length: 35	
name	Policy name.	string	Maximum length: 35	
policyid	Policy ID.	integer	Minimum value: 0 Maximum value: 9999	0
service <name>	Service name. Service name.	string	Maximum length: 79	
srcaddr <name>	Source address name. Address name.	string	Maximum length: 79	
status	Enable/disable access control list status.	option	-	enable
		Option	Description	
		enable	Enable access control list status.	
		disable	Disable access control list status.	

## config firewall address

Configure IPv4 addresses.

```

config firewall address
    Description: Configure IPv4 addresses.
    edit <name>
        set allow-routing [enable|disable]
        set associated-interface {string}
        set cache-ttl {integer}
        set clearpass-spt [unknown|healthy|...]
        set color {integer}
        set comment {var-string}
        set country {string}
        set end-ip {ipv4-address-any}
        set epq-name {string}
        set fabric-object [enable|disable]
        set filter {var-string}
        set fqdn {string}
        set fsso-group <name1>, <name2>, ...
        set interface {string}
    config list
        Description: IP address list.
        edit <ip>
            next
        end
        set macaddr <macaddr1>, <macaddr2>, ...
        set node-ip-only [enable|disable]
        set obj-id {var-string}
        set obj-tag {string}
        set obj-type [ip|mac]
        set organization {string}
        set policy-group {string}
        set sdn {string}
        set sdn-addr-type [private|public|...]
        set sdn-tag {string}
        set start-ip {ipv4-address-any}
        set sub-type [sdn|clearpass-spt|...]
        set subnet {ipv4-classnet-any}
        set subnet-name {string}
        set tag-detection-level {string}
        set tag-type {string}
    config tagging
        Description: Config object tagging.
        edit <name>
            set category {string}
            set tags <name1>, <name2>, ...
        next
    end
    set tenant {string}
    set type [ipmask|iprange|...]
    set uuid {uuid}
    set wildcard {ipv4-classnet-any}
    set wildcard-fqdn {string}
next
end

```

## config firewall address

Parameter	Description	Type	Size	Default														
allow-routing	Enable/disable use of this address in the static route configuration.	option	-	disable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable use of this address in the static route configuration.</td></tr><tr><td><i>disable</i></td><td>Disable use of this address in the static route configuration.</td></tr></table>	Option	Description	<i>enable</i>	Enable use of this address in the static route configuration.	<i>disable</i>	Disable use of this address in the static route configuration.											
	Option	Description																
	<i>enable</i>	Enable use of this address in the static route configuration.																
<i>disable</i>	Disable use of this address in the static route configuration.																	
associated-interface	Network interface associated with address.	string	Maximum length: 35															
cache-ttl	Defines the minimal TTL of individual IP addresses in FQDN cache measured in seconds.	integer	Minimum value: 0 Maximum value: 86400	0														
clearpass-spt	SPT (System Posture Token) value.	option	-	unknown														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>unknown</i></td><td>UNKNOWN.</td></tr><tr><td><i>healthy</i></td><td>HEALTHY.</td></tr><tr><td><i>quarantine</i></td><td>QUARANTINE.</td></tr><tr><td><i>checkup</i></td><td>CHECKUP.</td></tr><tr><td><i>transient</i></td><td>TRANSIENT.</td></tr><tr><td><i>infected</i></td><td>INFECTED.</td></tr></table>	Option	Description	<i>unknown</i>	UNKNOWN.	<i>healthy</i>	HEALTHY.	<i>quarantine</i>	QUARANTINE.	<i>checkup</i>	CHECKUP.	<i>transient</i>	TRANSIENT.	<i>infected</i>	INFECTED.			
	Option	Description																
	<i>unknown</i>	UNKNOWN.																
	<i>healthy</i>	HEALTHY.																
	<i>quarantine</i>	QUARANTINE.																
	<i>checkup</i>	CHECKUP.																
	<i>transient</i>	TRANSIENT.																
<i>infected</i>	INFECTED.																	
color	Color of icon on the GUI.	integer	Minimum value: 0 Maximum value: 32	0														
comment	Comment.	var-string	Maximum length: 255															
country	IP addresses associated to a specific country.	string	Maximum length: 2															
end-ip	Final IP address (inclusive) in the range for the address.	ipv4-address-any	Not Specified	0.0.0.0														
epg-name	Endpoint group name.	string	Maximum length: 255															

Parameter	Description	Type	Size	Default
fabric-object	Security Fabric global object setting.	option	-	disable
	Option	Description		
	enable	Object is set as a security fabric-wide global object.		
	disable	Object is local to this security fabric member.		
filter	Match criteria filter.	var-string	Maximum length: 2047	
fqdn	Fully Qualified Domain Name address.	string	Maximum length: 255	
fsso-group <name>	FSSO group(s). FSSO group name.	string	Maximum length: 511	
interface	Name of interface whose IP address is to be used.	string	Maximum length: 35	
macaddr <macaddr>	Multiple MAC address ranges. MAC address ranges <start>[-<end>] separated by space.	string	Maximum length: 127	
name	Address name.	string	Maximum length: 79	
node-ip-only	Enable/disable collection of node addresses only in Kubernetes.	option	-	disable
	Option	Description		
	enable	Enable collection of node addresses only in Kubernetes.		
	disable	Disable collection of node addresses only in Kubernetes.		
obj-id	Object ID for NSX.	var-string	Maximum length: 255	
obj-tag	Tag of dynamic address object.	string	Maximum length: 255	
obj-type	Object type.	option	-	ip
	Option	Description		
	ip	IP address.		
	mac	MAC address		
organization	Organization domain name (Syntax: organization/domain).	string	Maximum length: 35	

Parameter	Description	Type	Size	Default
policy-group	Policy group name.	string	Maximum length: 15	
sdn	SDN.	string	Maximum length: 35	
sdn-addr-type	Type of addresses to collect.	option	-	private
	<b>Option</b>	<b>Description</b>		
	<i>private</i>	Collect private addresses only.		
	<i>public</i>	Collect public addresses only.		
	<i>all</i>	Collect both public and private addresses.		
sdn-tag	SDN Tag.	string	Maximum length: 15	
start-ip	First IP address (inclusive) in the range for the address.	ipv4-address-any	Not Specified	0.0.0.0
sub-type	Sub-type of address.	option	-	sdn
	<b>Option</b>	<b>Description</b>		
	<i>sdn</i>	SDN address.		
	<i>clearpass-spt</i>	ClearPass SPT (System Posture Token) address.		
	<i>fsso</i>	FSSO address.		
	<i>ems-tag</i>	FortiClient EMS tag.		
	<i>fortivoice-tag</i>	FortiVoice tag.		
	<i>fortinac-tag</i>	FortiNAC tag.		
	<i>swc-tag</i>	Switch Controller NAC policy tag.		
subnet	IP address and subnet mask of address.	ipv4-classnet-any	Not Specified	0.0.0.0 0.0.0.0
subnet-name	Subnet name.	string	Maximum length: 255	
tag-detection-level	Tag detection level of dynamic address object.	string	Maximum length: 15	
tag-type	Tag type of dynamic address object.	string	Maximum length: 63	

Parameter	Description	Type	Size	Default
tenant	Tenant.	string	Maximum length: 35	
type	Type of address.	option	-	ipmask
	Option	Description		
	ipmask	Standard IPv4 address with subnet mask.		
	iprange	Range of IPv4 addresses between two specified addresses (inclusive).		
	fqdn	Fully Qualified Domain Name address.		
	geography	IP addresses from a specified country.		
	wildcard	Standard IPv4 using a wildcard subnet mask.		
	dynamic	Dynamic address object.		
	interface-subnet	IP and subnet of interface.		
	mac	Range of MAC addresses.		
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000
wildcard	IP address and wildcard netmask.	ipv4-classnet-any	Not Specified	0.0.0.0 0.0.0.0
wildcard-fqdn	Fully Qualified Domain Name with wildcard characters.	string	Maximum length: 255	

## config list

Parameter	Description	Type	Size	Default
ip	IP.	string	Maximum length: 35	

## config tagging

Parameter	Description	Type	Size	Default
name	Tagging entry name.	string	Maximum length: 63	
category	Tag category.	string	Maximum length: 63	
tags <name>	Tags. Tag name.	string	Maximum length: 79	



## config firewall address6-template

Configure IPv6 address templates.

```
config firewall address6-template
  Description: Configure IPv6 address templates.
  edit <name>
    set fabric-object [enable|disable]
    set ip6 {ipv6-network}
    config subnet-segment
      Description: IPv6 subnet segments.
      edit <id>
        set name {string}
        set bits {integer}
        set exclusive [enable|disable]
        config values
          Description: Subnet segment values.
          edit <name>
            set value {string}
          next
        end
      next
    end
  set subnet-segment-count {integer}
next
end
```

## config firewall address6-template

Parameter	Description	Type	Size	Default
fabric-object	Security Fabric global object setting.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Object is set as a security fabric-wide global object.		
	<i>disable</i>	Object is local to this security fabric member.		
ip6	IPv6 address prefix.	ipv6-network	Not Specified	::/0
name	IPv6 address template name.	string	Maximum length: 63	
subnet-segment-count	Number of IPv6 subnet segments.	integer	Minimum value: 1 Maximum value: 6	0

## config subnet-segment

Parameter	Description	Type	Size	Default
id	Subnet segment ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
name	Subnet segment name.	string	Maximum length: 63	
bits	Number of bits.	integer	Minimum value: 1 Maximum value: 16	0
exclusive	Enable/disable exclusive value.	option	-	disable
		Option	Description	
		<i>enable</i>	Enable exclusive value.	
		<i>disable</i>	Disable exclusive value.	

## config values

Parameter	Description	Type	Size	Default
name	Subnet segment value name.	string	Maximum length: 63	
value	Subnet segment value.	string	Maximum length: 35	

## config firewall address6

Configure IPv6 firewall addresses.

```
config firewall address6
  Description: Configure IPv6 firewall addresses.
  edit <name>
    set cache-ttl {integer}
    set color {integer}
    set comment {var-string}
    set country {string}
    set end-ip {ipv6-address}
    set fabric-object [enable|disable]
    set fqdn {string}
    set host {ipv6-address}
    set host-type [any|specific]
    set ip6 {ipv6-network}
```

```

config list
    Description: IP address list.
    edit <ip>
    next
end
set macaddr <macaddr1>, <macaddr2>, ...
set obj-id {var-string}
set sdn {string}
set start-ip {ipv6-address}
config subnet-segment
    Description: IPv6 subnet segments.
    edit <name>
        set type [any|specific]
        set value {string}
    next
end
config tagging
    Description: Config object tagging.
    edit <name>
        set category {string}
        set tags <name1>, <name2>, ...
    next
end
set template {string}
set type [ipprefix|iprange|...]
set uuid {uuid}
next
end

```

## config firewall address6

Parameter	Description	Type	Size	Default
cache-ttl	Minimal TTL of individual IPv6 addresses in FQDN cache.	integer	Minimum value: 0 Maximum value: 86400	0
color	Integer value to determine the color of the icon in the GUI.	integer	Minimum value: 0 Maximum value: 32	0
comment	Comment.	var-string	Maximum length: 255	
country	IPv6 addresses associated to a specific country.	string	Maximum length: 2	
end-ip	Final IP address (inclusive) in the range for the address (format: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx).	ipv6-address	Not Specified	::

Parameter	Description	Type	Size	Default						
fabric-object	Security Fabric global object setting.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Object is set as a security fabric-wide global object.</td></tr><tr><td>disable</td><td>Object is local to this security fabric member.</td></tr></table>				Option	Description	enable	Object is set as a security fabric-wide global object.	disable	Object is local to this security fabric member.
	Option	Description								
	enable	Object is set as a security fabric-wide global object.								
disable	Object is local to this security fabric member.									
fqdn	Fully qualified domain name.	string	Maximum length: 255							
host	Host Address.	ipv6-address	Not Specified	::						
host-type	Host type.	option	-	any						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>any</td><td>Wildcard.</td></tr><tr><td>specific</td><td>Specific host address.</td></tr></table>				Option	Description	any	Wildcard.	specific	Specific host address.
	Option	Description								
	any	Wildcard.								
specific	Specific host address.									
ip6	IPv6 address prefix (format: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/xxx).	ipv6-network	Not Specified	::/0						
macaddr <macaddr>	Multiple MAC address ranges. MAC address ranges <start>[-<end>] separated by space.	string	Maximum length: 127							
name	Address name.	string	Maximum length: 79							
obj-id	Object ID for NSX.	var-string	Maximum length: 255							
sdn	SDN.	string	Maximum length: 35							
start-ip	First IP address (inclusive) in the range for the address (format: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx).	ipv6-address	Not Specified	::						
template	IPv6 address template.	string	Maximum length: 63							
type	Type of IPv6 address object.	option	-	ipprefix						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ipprefix</td><td>Uses the IP prefix to define a range of IPv6 addresses.</td></tr><tr><td>iprange</td><td>Range of IPv6 addresses between two specified addresses (inclusive).</td></tr></table>				Option	Description	ipprefix	Uses the IP prefix to define a range of IPv6 addresses.	iprange	Range of IPv6 addresses between two specified addresses (inclusive).
	Option	Description								
	ipprefix	Uses the IP prefix to define a range of IPv6 addresses.								
iprange	Range of IPv6 addresses between two specified addresses (inclusive).									

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>fqdn</i>	Fully qualified domain name.		
	<i>geography</i>	IPv6 addresses from a specified country.		
	<i>dynamic</i>	Dynamic address object for SDN.		
	<i>template</i>	Template.		
	<i>mac</i>	Range of MAC addresses.		
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000

### config list

Parameter	Description	Type	Size	Default
ip	IP.	string	Maximum length: 89	

### config subnet-segment

Parameter	Description	Type	Size	Default
name	Name.	string	Maximum length: 63	
type	Subnet segment type.	option	-	any
	<b>Option</b>	<b>Description</b>		
	<i>any</i>	Wildcard.		
	<i>specific</i>	Specific subnet segment address.		
value	Subnet segment value.	string	Maximum length: 35	

### config tagging

Parameter	Description	Type	Size	Default
name	Tagging entry name.	string	Maximum length: 63	
category	Tag category.	string	Maximum length: 63	

Parameter	Description	Type	Size	Default
tags <name>	Tags. Tag name.	string	Maximum length: 79	

## config firewall addrgrp

Configure IPv4 address groups.

```
config firewall addrgrp
  Description: Configure IPv4 address groups.
  edit <name>
    set allow-routing [enable|disable]
    set category [default|ztna-ems-tag|...]
    set color {integer}
    set comment {var-string}
    set exclude [enable|disable]
    set exclude-member <name1>, <name2>, ...
    set fabric-object [enable|disable]
    set member <name1>, <name2>, ...
    config tagging
      Description: Config object tagging.
      edit <name>
        set category {string}
        set tags <name1>, <name2>, ...
      next
    next
  end
  set type [default|folder]
  set uuid {uuid}
next
end
```

## config firewall addrgrp

Parameter	Description	Type	Size	Default						
allow-routing	Enable/disable use of this group in the static route configuration.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable use of this group in the static route configuration.</td></tr><tr><td><i>disable</i></td><td>Disable use of this group in the static route configuration.</td></tr></table>	Option	Description	<i>enable</i>	Enable use of this group in the static route configuration.	<i>disable</i>	Disable use of this group in the static route configuration.			
Option	Description									
<i>enable</i>	Enable use of this group in the static route configuration.									
<i>disable</i>	Disable use of this group in the static route configuration.									
category	Address group category.	option	-	default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>Default address group category (cannot be used as ztna-ems-tag/ztna-geo-tag in policy).</td></tr></table>	Option	Description	<i>default</i>	Default address group category (cannot be used as ztna-ems-tag/ztna-geo-tag in policy).					
Option	Description									
<i>default</i>	Default address group category (cannot be used as ztna-ems-tag/ztna-geo-tag in policy).									

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ztna-ems-tag</i></td><td>Members must be ztna-ems-tag group or ems-tag address, can be used as ztna-ems-tag in policy.</td></tr><tr><td><i>ztna-geo-tag</i></td><td>Members must be ztna-geo-tag group or geographic address, can be used as ztna-geo-tag in policy.</td></tr></table>				Option	Description	<i>ztna-ems-tag</i>	Members must be ztna-ems-tag group or ems-tag address, can be used as ztna-ems-tag in policy.	<i>ztna-geo-tag</i>	Members must be ztna-geo-tag group or geographic address, can be used as ztna-geo-tag in policy.
	Option	Description								
	<i>ztna-ems-tag</i>	Members must be ztna-ems-tag group or ems-tag address, can be used as ztna-ems-tag in policy.								
<i>ztna-geo-tag</i>	Members must be ztna-geo-tag group or geographic address, can be used as ztna-geo-tag in policy.									
color	Color of icon on the GUI.	integer	Minimum value: 0 Maximum value: 32	0						
comment	Comment.	var-string	Maximum length: 255							
exclude	Enable/disable address exclusion.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable address exclusion.</td></tr><tr><td><i>disable</i></td><td>Disable address exclusion.</td></tr></table>				Option	Description	<i>enable</i>	Enable address exclusion.	<i>disable</i>	Disable address exclusion.
	Option	Description								
	<i>enable</i>	Enable address exclusion.								
<i>disable</i>	Disable address exclusion.									
exclude-member <name>	Address exclusion member. Address name.	string	Maximum length: 79							
fabric-object	Security Fabric global object setting.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Object is set as a security fabric-wide global object.</td></tr><tr><td><i>disable</i></td><td>Object is local to this security fabric member.</td></tr></table>				Option	Description	<i>enable</i>	Object is set as a security fabric-wide global object.	<i>disable</i>	Object is local to this security fabric member.
	Option	Description								
	<i>enable</i>	Object is set as a security fabric-wide global object.								
<i>disable</i>	Object is local to this security fabric member.									
member <name>	Address objects contained within the group. Address name.	string	Maximum length: 79							
name	Address group name.	string	Maximum length: 79							
type	Address group type.	option	-	default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>Default address group type (address may belong to multiple groups).</td></tr><tr><td><i>folder</i></td><td>Address folder group (members may not belong to any other group).</td></tr></table>				Option	Description	<i>default</i>	Default address group type (address may belong to multiple groups).	<i>folder</i>	Address folder group (members may not belong to any other group).
	Option	Description								
	<i>default</i>	Default address group type (address may belong to multiple groups).								
<i>folder</i>	Address folder group (members may not belong to any other group).									
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000						

## config tagging

Parameter	Description	Type	Size	Default
name	Tagging entry name.	string	Maximum length: 63	
category	Tag category.	string	Maximum length: 63	
tags <name>	Tags. Tag name.	string	Maximum length: 79	

## config firewall addrgrp6

Configure IPv6 address groups.

```
config firewall addrgrp6
  Description: Configure IPv6 address groups.
  edit <name>
    set color {integer}
    set comment {var-string}
    set fabric-object [enable|disable]
    set member <name1>, <name2>, ...
    config tagging
      Description: Config object tagging.
      edit <name>
        set category {string}
        set tags <name1>, <name2>, ...
      next
    end
    set uuid {uuid}
  next
end
```

## config firewall addrgrp6

Parameter	Description	Type	Size	Default
color	Integer value to determine the color of the icon in the GUI.	integer	Minimum value: 0 Maximum value: 32	0
comment	Comment.	var-string	Maximum length: 255	
fabric-object	Security Fabric global object setting.	option	-	disable



Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Object is set as a security fabric-wide global object.		
	<i>disable</i>	Object is local to this security fabric member.		
member <name>	Address objects contained within the group. Address6/addrgrp6 name.	string	Maximum length: 79	
name	IPv6 address group name.	string	Maximum length: 79	
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000

### config tagging

Parameter	Description	Type	Size	Default
name	Tagging entry name.	string	Maximum length: 63	
category	Tag category.	string	Maximum length: 63	
tags <name>	Tags. Tag name.	string	Maximum length: 79	

## config firewall auth-portal

Configure firewall authentication portals.

```
config firewall auth-portal
    Description: Configure firewall authentication portals.
    set groups <name1>, <name2>, ...
    set identity-based-route {string}
    set portal-addr {string}
    set portal-addr6 {string}
end
```

### config firewall auth-portal

Parameter	Description	Type	Size	Default
groups <name>	Firewall user groups permitted to authenticate through this portal. Separate group names with spaces. Group name.	string	Maximum length: 79	

Parameter	Description	Type	Size	Default
identity-based-route	Name of the identity-based route that applies to this portal.	string	Maximum length: 35	
portal-addr	Address (or FQDN) of the authentication portal.	string	Maximum length: 63	
portal-addr6	IPv6 address (or FQDN) of authentication portal.	string	Maximum length: 63	

## config firewall central-snat-map

Configure IPv4 and IPv6 central SNAT policies.

```
config firewall central-snat-map
    Description: Configure IPv4 and IPv6 central SNAT policies.
    edit <policyid>
        set comments {var-string}
        set dst-addr <name1>, <name2>, ...
        set dst-addr6 <name1>, <name2>, ...
        set dstintf <name1>, <name2>, ...
        set nat [disable|enable]
        set nat-ippool <name1>, <name2>, ...
        set nat-ippool6 <name1>, <name2>, ...
        set nat-port {user}
        set nat46 [enable|disable]
        set nat64 [enable|disable]
        set orig-addr <name1>, <name2>, ...
        set orig-addr6 <name1>, <name2>, ...
        set orig-port {user}
        set protocol {integer}
        set srcintf <name1>, <name2>, ...
        set status [enable|disable]
        set type [ipv4|ipv6]
        set uuid {uuid}
    next
end
```

## config firewall central-snat-map

Parameter	Description	Type	Size	Default
comments	Comment.	var-string	Maximum length: 1023	
dst-addr <name>	IPv4 Destination address. Address name.	string	Maximum length: 79	
dst-addr6 <name>	IPv6 Destination address. Address name.	string	Maximum length: 79	

Parameter	Description	Type	Size	Default						
dstintf <name>	Destination interface name from available interfaces. Interface name.	string	Maximum length: 79							
nat	Enable/disable source NAT.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable source NAT.</td></tr><tr><td>enable</td><td>Enable source NAT.</td></tr></table>	Option	Description	disable	Disable source NAT.	enable	Enable source NAT.			
Option	Description									
disable	Disable source NAT.									
enable	Enable source NAT.									
nat-ippool <name>	Name of the IP pools to be used to translate addresses from available IP Pools. IP pool name.	string	Maximum length: 79							
nat-ippool6 <name>	IPv6 pools to be used for source NAT. IPv6 pool name.	string	Maximum length: 79							
nat-port	Translated port or port range (1 to 65535, 0 means any port).	user	Not Specified							
nat46	Enable/disable NAT46.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable NAT46.</td></tr><tr><td>disable</td><td>Disable NAT46.</td></tr></table>	Option	Description	enable	Enable NAT46.	disable	Disable NAT46.			
Option	Description									
enable	Enable NAT46.									
disable	Disable NAT46.									
nat64	Enable/disable NAT64.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable NAT64.</td></tr><tr><td>disable</td><td>Disable NAT64.</td></tr></table>	Option	Description	enable	Enable NAT64.	disable	Disable NAT64.			
Option	Description									
enable	Enable NAT64.									
disable	Disable NAT64.									
orig-addr <name>	IPv4 Original address. Address name.	string	Maximum length: 79							
orig-addr6 <name>	IPv6 Original address. Address name.	string	Maximum length: 79							
orig-port	Original TCP port (1 to 65535, 0 means any port).	user	Not Specified							
policyid	Policy ID.	integer	Minimum value: 0 Maximum value: 4294967295	0						

Parameter	Description	Type	Size	Default						
protocol	Integer value for the protocol type.	integer	Minimum value: 0 Maximum value: 255	0						
srcintf <name>	Source interface name from available interfaces. Interface name.	string	Maximum length: 79							
status	Enable/disable the active status of this policy.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable this policy.</td></tr><tr><td><i>disable</i></td><td>Disable this policy.</td></tr></table>				Option	Description	<i>enable</i>	Enable this policy.	<i>disable</i>	Disable this policy.
Option	Description									
<i>enable</i>	Enable this policy.									
<i>disable</i>	Disable this policy.									
type	IPv4/IPv6 source NAT.	option	-	ipv4						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ipv4</i></td><td>Perform IPv4 source NAT.</td></tr><tr><td><i>ipv6</i></td><td>Perform IPv6 source NAT.</td></tr></table>				Option	Description	<i>ipv4</i>	Perform IPv4 source NAT.	<i>ipv6</i>	Perform IPv6 source NAT.
Option	Description									
<i>ipv4</i>	Perform IPv4 source NAT.									
<i>ipv6</i>	Perform IPv6 source NAT.									
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000						

## config firewall city

Define city table.

```
config firewall city
    Description: Define city table.
    edit <id>
        set name {string}
    next
end
```

## config firewall city

Parameter	Description	Type	Size	Default
id	City ID.	integer	Minimum value: 0 Maximum value: 65535	0
name	City name.	string	Maximum length: 63	

## config firewall country

Define country table.

```
config firewall country
    Description: Define country table.
    edit <id>
        set name {string}
        set region <id1>, <id2>, ...
    next
end
```

## config firewall country

Parameter	Description	Type	Size	Default
id	Country ID.	integer	Minimum value: 0 Maximum value: 65535	0
name	Country name.	string	Maximum length: 63	
region <id>	Region ID list. Region ID.	integer	Minimum value: 0 Maximum value: 65535	

## config firewall decrypted-traffic-mirror

Configure decrypted traffic mirror.

```
config firewall decrypted-traffic-mirror
    Description: Configure decrypted traffic mirror.
    edit <name>
        set dstmac {mac-address}
        set interface <name1>, <name2>, ...
        set traffic-source [client|server|...]
        set traffic-type {option1}, {option2}, ...
    next
end
```

## config firewall decrypted-traffic-mirror

Parameter	Description	Type	Size	Default								
dstmac	Set destination MAC address for mirrored traffic.	mac-address	Not Specified	ff:ff:ff:ff:ff:ff								
interface <name>	Decrypted traffic mirror interface. Decrypted traffic mirror interface.	string	Maximum length: 79									
name	Name.	string	Maximum length: 35									
traffic-source	Source of decrypted traffic to be mirrored.	option	-	client								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>client</td><td>Mirror client side decrypted traffic.</td></tr><tr><td>server</td><td>Mirror server side decrypted traffic.</td></tr><tr><td>both</td><td>Mirror both client and server side decrypted traffic.</td></tr></table>				Option	Description	client	Mirror client side decrypted traffic.	server	Mirror server side decrypted traffic.	both	Mirror both client and server side decrypted traffic.
Option	Description											
client	Mirror client side decrypted traffic.											
server	Mirror server side decrypted traffic.											
both	Mirror both client and server side decrypted traffic.											
traffic-type	Types of decrypted traffic to be mirrored.	option	-	ssl								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ssl</td><td>Mirror decrypted SSL traffic.</td></tr><tr><td>ssh</td><td>Mirror decrypted SSH traffic.</td></tr></table>				Option	Description	ssl	Mirror decrypted SSL traffic.	ssh	Mirror decrypted SSH traffic.		
Option	Description											
ssl	Mirror decrypted SSL traffic.											
ssh	Mirror decrypted SSH traffic.											

## config firewall dnstranslation

Configure DNS translation.

```
config firewall dnstranslation
  Description: Configure DNS translation.
  edit <id>
    set dst {ipv4-address}
    set netmask {ipv4-netmask}
    set src {ipv4-address}
  next
end
```

## config firewall dnstranslation

Parameter	Description	Type	Size	Default
dst	IPv4 address or subnet on the external network to substitute for the resolved address in DNS query replies. Can be single IP address or subnet on the external network, but number of addresses must equal number of mapped IP addresses in src.	ipv4-address	Not Specified	0.0.0.0
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
netmask	If src and dst are subnets rather than single IP addresses, enter the netmask for both src and dst.	ipv4-netmask	Not Specified	255.255.255.255
src	IPv4 address or subnet on the internal network to compare with the resolved address in DNS query replies. If the resolved address matches, the resolved address is substituted with dst.	ipv4-address	Not Specified	0.0.0.0

## config firewall gtp



This command is available for model(s): FortiGate 2600F, FortiGate 3000F, FortiGate 3001F, FortiGate 3400E.

It is not available for: FortiGate 1000D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2601F, FortiGate 3000D, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

### Configure GTP.

```
config firewall gtp
  Description: Configure GTP.
  edit <name>
    set addr-notify {ipv4-address-any}
    config apn
      Description: APN.
      edit <id>
        set apnmember <name1>, <name2>, ...
        set action [allow|deny]
        set selection-mode {option1}, {option2}, ...
      next
    end
    set apn-filter [enable|disable]
    set authorized-ggsns {string}
    set authorized-ggsns6 {string}
    set authorized-sgsns {string}
    set authorized-sgsns6 {string}
    set comment {var-string}
    set context-id {integer}
    set control-plane-message-rate-limit {integer}
    set default-apn-action [allow|deny]
    set default-imsi-action [allow|deny]
    set default-ip-action [allow|deny]
    set default-noip-action [allow|deny]
    set default-policy-action [allow|deny]
```



```

set denied-log [enable|disable]
set echo-request-interval {integer}
set extension-log [enable|disable]
set forwarded-log [enable|disable]
set global-tunnel-limit {string}
set gtp-in-gtp [allow|deny]
set gtpu-denied-log [enable|disable]
set gtpu-forwarded-log [enable|disable]
set gtpu-log-freq {integer}
set half-close-timeout {integer}
set half-open-timeout {integer}
set handover-group {string}
set handover-group6 {string}
set ie-allow-list-v0v1 {string}
set ie-allow-list-v2 {string}
config ie-remove-policy
    Description: IE remove policy.
    edit <id>
        set sgsn-addr {string}
        set sgsn-addr6 {string}
        set remove-ies {option1}, {option2}, ...
    next
end
set ie-remover [enable|disable]
config ie-validation
    Description: IE validation.
    set imsi [enable|disable]
    set rai [enable|disable]
    set reordering-required [enable|disable]
    set ms-validated [enable|disable]
    set selection-mode [enable|disable]
    set nsapi [enable|disable]
    set charging-ID [enable|disable]
    set end-user-addr [enable|disable]
    set mm-context [enable|disable]
    set pdp-context [enable|disable]
    set gsn-addr [enable|disable]
    set msisdn [enable|disable]
    set qos-profile [enable|disable]
    set apn-restriction [enable|disable]
    set rat-type [enable|disable]
    set uli [enable|disable]
    set ms-tzone [enable|disable]
    set imei [enable|disable]
    set charging-gateway-addr [enable|disable]
end
config imsi
    Description: IMSI.
    edit <id>
        set mcc-mnc {string}
        set msisdn-prefix {string}
        set apnmember <name1>, <name2>, ...
        set action [allow|deny]
        set selection-mode {option1}, {option2}, ...
    next
end

```

```

set imsi-filter [enable|disable]
set interface-notify {string}
set invalid-reserved-field [allow|deny]
set invalid-sgsns-to-log {string}
set invalid-sgsns6-to-log {string}
set ip-filter [enable|disable]
config ip-policy
    Description: IP policy.
    edit <id>
        set srcaddr {string}
        set dstaddr {string}
        set srcaddr6 {string}
        set dstaddr6 {string}
        set action [allow|deny]
    next
end
set log-freq {integer}
set log-gtpu-limit {integer}
set log-imsi-prefix {string}
set log-msisdn-prefix {string}
set max-message-length {integer}
set message-filter-v0v1 {string}
set message-filter-v2 {string}
config message-rate-limit
    Description: Message rate limiting.
    set echo-request {integer}
    set echo-reponse {integer}
    set version-not-support {integer}
    set create-pdp-request {integer}
    set create-pdp-response {integer}
    set update-pdp-request {integer}
    set update-pdp-response {integer}
    set delete-pdp-request {integer}
    set delete-pdp-response {integer}
    set create-aa-pdp-request {integer}
    set create-aa-pdp-response {integer}
    set delete-aa-pdp-request {integer}
    set delete-aa-pdp-response {integer}
    set error-indication {integer}
    set pdu-notify-request {integer}
    set pdu-notify-response {integer}
    set pdu-notify-rej-request {integer}
    set pdu-notify-rej-response {integer}
    set support-ext-hdr-notify {integer}
    set send-route-request {integer}
    set send-route-response {integer}
    set failure-report-request {integer}
    set failure-report-response {integer}
    set note-ms-request {integer}
    set note-ms-response {integer}
    set identification-request {integer}
    set identification-response {integer}
    set sgsn-context-request {integer}
    set sgsn-context-response {integer}
    set sgsn-context-ack {integer}
    set fwd-relocation-request {integer}

```

```

    set fwd-relocation-response {integer}
    set fwd-relocation-complete {integer}
    set relocation-cancel-request {integer}
    set relocation-cancel-response {integer}
    set fwd-srns-context {integer}
    set fwd-reloc-complete-ack {integer}
    set fwd-srns-context-ack {integer}
    set ran-info {integer}
    set mbms-notify-request {integer}
    set mbms-notify-response {integer}
    set mbms-notify-rej-request {integer}
    set mbms-notify-rej-response {integer}
    set create-mbms-request {integer}
    set create-mbms-response {integer}
    set update-mbms-request {integer}
    set update-mbms-response {integer}
    set delete-mbms-request {integer}
    set delete-mbms-response {integer}
    set mbms-reg-request {integer}
    set mbms-reg-response {integer}
    set mbms-de-reg-request {integer}
    set mbms-de-reg-response {integer}
    set mbms-ses-start-request {integer}
    set mbms-ses-start-response {integer}
    set mbms-ses-stop-request {integer}
    set mbms-ses-stop-response {integer}
    set g-pdu {integer}
end
config message-rate-limit-v0
    Description: Message rate limiting for GTP version 0.
    set echo-request {integer}
    set create-pdp-request {integer}
    set delete-pdp-request {integer}
end
config message-rate-limit-v1
    Description: Message rate limiting for GTP version 1.
    set echo-request {integer}
    set create-pdp-request {integer}
    set delete-pdp-request {integer}
end
config message-rate-limit-v2
    Description: Message rate limiting for GTP version 2.
    set echo-request {integer}
    set create-session-request {integer}
    set delete-session-request {integer}
end
set min-message-length {integer}
set miss-must-ie [allow|deny]
set monitor-mode [enable|disable|...]
set noip-filter [enable|disable]
config noip-policy
    Description: No IP policy.
    edit <id>
        set type [etsi|ietf]
        set start {integer}
        set end {integer}

```

```

        set action [allow|deny]
    next
end
set out-of-state-ie [allow|deny]
set out-of-state-message [allow|deny]
config per-apn-shaper
    Description: Per APN shaper.
    edit <id>
        set apn {string}
        set version {integer}
        set rate-limit {integer}
    next
end
config policy
    Description: Policy.
    edit <id>
        set apnmember <name1>, <name2>, ...
        set messages {option1}, {option2}, ...
        set apn-sel-mode {option1}, {option2}, ...
        set max-apn-restriction [all|public-1|...]
        set imsi-prefix {string}
        set msisdn-prefix {string}
        set rat-type {option1}, {option2}, ...
        set imei {string}
        set action [allow|deny]
        set rai {string}
        set uli {string}
    next
end
set policy-filter [enable|disable]
config policy-v2
    Description: Apply allow or deny action to each GTPv2-c packet.
    edit <id>
        set apnmember <name1>, <name2>, ...
        set messages {option1}, {option2}, ...
        set apn-sel-mode {option1}, {option2}, ...
        set max-apn-restriction [all|public-1|...]
        set imsi-prefix {string}
        set msisdn-prefix {string}
        set rat-type {option1}, {option2}, ...
        set mei {string}
        set action [allow|deny]
        set uli {string}
    next
end
set port-notify {integer}
set rat-timeout-profile {string}
set rate-limit-mode [per-profile|per-stream|...]
set rate-limited-log [enable|disable]
set rate-sampling-interval {integer}
set remove-if-echo-expires [enable|disable]
set remove-if-recovery-differ [enable|disable]
set reserved-ie [allow|deny]
set send-delete-when-timeout [enable|disable]
set send-delete-when-timeout-v2 [enable|disable]
set spoof-src-addr [allow|deny]

```

```

set state-invalid-log [enable|disable]
set sub-second-interval [0.5|0.25|...]
set sub-second-sampling [enable|disable]
set traffic-count-log [enable|disable]
set tunnel-limit {integer}
set tunnel-limit-log [enable|disable]
set tunnel-timeout {integer}
set unknown-version-action [allow|deny]
set user-plane-message-rate-limit {integer}
set warning-threshold {integer}

```

```

next

```

```

end

```

## config firewall gtp

Parameter	Description	Type	Size	Default
addr-notify	overbilling notify address	ipv4-address-any	Not Specified	0.0.0.0
apn-filter	apn filter	option	-	disable
	Option	Description		
	enable	Enable setting.		
	disable	Disable setting.		
authorized-ggsns	Authorized GGSN/PGW group.	string	Maximum length: 79	
authorized-ggsns6	Authorized GGSN/PGW IPv6 group.	string	Maximum length: 79	
authorized-sgsns	Authorized SGSN/SGW group.	string	Maximum length: 79	
authorized-sgsns6	Authorized SGSN/SGW IPv6 group.	string	Maximum length: 79	
comment	Comment.	var-string	Maximum length: 255	
context-id	Overbilling context.	integer	Minimum value: 0 Maximum value: 4294967295	696

Parameter	Description	Type	Size	Default						
control-plane-message-rate-limit	control plane message rate limit	integer	Minimum value: 0 Maximum value: 4294967295	0						
default-apn-action	default apn action	option	-	allow						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow setting.</td></tr><tr><td><i>deny</i></td><td>Deny setting.</td></tr></table>	Option	Description	<i>allow</i>	Allow setting.	<i>deny</i>	Deny setting.			
Option	Description									
<i>allow</i>	Allow setting.									
<i>deny</i>	Deny setting.									
default-imsi-action	default imsi action	option	-	allow						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow setting.</td></tr><tr><td><i>deny</i></td><td>Deny setting.</td></tr></table>	Option	Description	<i>allow</i>	Allow setting.	<i>deny</i>	Deny setting.			
Option	Description									
<i>allow</i>	Allow setting.									
<i>deny</i>	Deny setting.									
default-ip-action	default action for encapsulated IP traffic	option	-	allow						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow setting.</td></tr><tr><td><i>deny</i></td><td>Deny setting.</td></tr></table>	Option	Description	<i>allow</i>	Allow setting.	<i>deny</i>	Deny setting.			
Option	Description									
<i>allow</i>	Allow setting.									
<i>deny</i>	Deny setting.									
default-noip-action	default action for encapsulated non-IP traffic	option	-	allow						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow setting.</td></tr><tr><td><i>deny</i></td><td>Deny setting.</td></tr></table>	Option	Description	<i>allow</i>	Allow setting.	<i>deny</i>	Deny setting.			
Option	Description									
<i>allow</i>	Allow setting.									
<i>deny</i>	Deny setting.									
default-policy-action	default advanced policy action	option	-	allow						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow setting.</td></tr><tr><td><i>deny</i></td><td>Deny setting.</td></tr></table>	Option	Description	<i>allow</i>	Allow setting.	<i>deny</i>	Deny setting.			
Option	Description									
<i>allow</i>	Allow setting.									
<i>deny</i>	Deny setting.									
denied-log	log denied	option	-	disable						

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
echo-request-interval	echo request interval (in seconds)	integer	Minimum value: 0 Maximum value: 4294967295	0
extension-log	log in extension format	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
forwarded-log	log forwarded	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
global-tunnel-limit	Global tunnel limit.	string	Maximum length: 63	
gtp-in-gtp	gtp in gtp	option	-	allow
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow setting.		
	<i>deny</i>	Deny setting.		
gtpu-denied-log	Enable/disable logging of denied GTP-U packets.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
gtpu-forwarded-log	Enable/disable logging of forwarded GTP-U packets.	option	-	disable

Parameter	Description	Type	Size	Default
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
gtpu-log-freq	Logging of frequency of GTP-U packets.	integer	Minimum value: 0 Maximum value: 4294967295	0
half-close-timeout	Half-close tunnel timeout (in seconds).	integer	Minimum value: 1 Maximum value: 30	10
half-open-timeout	Half-open tunnel timeout (in seconds).	integer	Minimum value: 1 Maximum value: 300	300
handover-group	Handover SGSN/SGW group.	string	Maximum length: 79	
handover-group6	Handover SGSN/SGW IPv6 group.	string	Maximum length: 79	
ie-allow-list-v0v1	IE allow list.	string	Maximum length: 63	
ie-allow-list-v2	IE allow list.	string	Maximum length: 63	
ie-remover	IE removal policy.	option	-	disable
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
imsi-filter	imsi filter	option	-	disable
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
interface-notify	overbilling interface	string	Maximum length: 15	



Parameter	Description	Type	Size	Default						
invalid-reserved-field	Invalid reserved field in GTP header	option	-	deny						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow setting.</td></tr><tr><td><i>deny</i></td><td>Deny setting.</td></tr></table>				Option	Description	<i>allow</i>	Allow setting.	<i>deny</i>	Deny setting.
	Option	Description								
	<i>allow</i>	Allow setting.								
<i>deny</i>	Deny setting.									
invalid-sgsns-to-log	Invalid SGSN group to be logged	string	Maximum length: 79							
invalid-sgsns6-to-log	Invalid SGSN IPv6 group to be logged.	string	Maximum length: 79							
ip-filter	IP filter for encapsulated traffic	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>				Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.
	Option	Description								
	<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.									
log-freq	Logging of frequency of GTP-C packets.	integer	Minimum value: 0 Maximum value: 4294967295	0						
log-gtpu-limit	the user data log limit	integer	Minimum value: 0 Maximum value: 512	0						
log-imsi-prefix	IMSI prefix for selective logging.	string	Maximum length: 15							
log-msisdn-prefix	the msisdn prefix for selective logging	string	Maximum length: 15							
max-message-length	max message length	integer	Minimum value: 0 Maximum value: 4294967295	1452						
message-filter-v0v1	Message filter.	string	Maximum length: 63							
message-filter-v2	Message filter.	string	Maximum length: 63							

Parameter	Description	Type	Size	Default								
min-message-length	min message length	integer	Minimum value: 0 Maximum value: 4294967295	0								
miss-must-ie	Missing mandatory information element	option	-	deny								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow setting.</td></tr><tr><td><i>deny</i></td><td>Deny setting.</td></tr></table>	Option	Description	<i>allow</i>	Allow setting.	<i>deny</i>	Deny setting.					
Option	Description											
<i>allow</i>	Allow setting.											
<i>deny</i>	Deny setting.											
monitor-mode	GTP monitor mode.	option	-	vdom								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable GTP monitor mode.</td></tr><tr><td><i>disable</i></td><td>Disable GTP monitor mode.</td></tr><tr><td><i>vdom</i></td><td>Enable/disable GTP monitor mode based on VDOM setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable GTP monitor mode.	<i>disable</i>	Disable GTP monitor mode.	<i>vdom</i>	Enable/disable GTP monitor mode based on VDOM setting.			
Option	Description											
<i>enable</i>	Enable GTP monitor mode.											
<i>disable</i>	Disable GTP monitor mode.											
<i>vdom</i>	Enable/disable GTP monitor mode based on VDOM setting.											
name	Profile name.	string	Maximum length: 63									
noip-filter	non-IP filter for encapsulated traffic	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
out-of-state-ie	Out of state information element.	option	-	deny								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow setting.</td></tr><tr><td><i>deny</i></td><td>Deny setting.</td></tr></table>	Option	Description	<i>allow</i>	Allow setting.	<i>deny</i>	Deny setting.					
Option	Description											
<i>allow</i>	Allow setting.											
<i>deny</i>	Deny setting.											
out-of-state-message	Out of state GTP message	option	-	deny								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow setting.</td></tr><tr><td><i>deny</i></td><td>Deny setting.</td></tr></table>	Option	Description	<i>allow</i>	Allow setting.	<i>deny</i>	Deny setting.					
Option	Description											
<i>allow</i>	Allow setting.											
<i>deny</i>	Deny setting.											
policy-filter	Advanced policy filter	option	-	disable								

Parameter	Description	Type	Size	Default
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
port-notify	overbilling notify port	integer	Minimum value: 0 Maximum value: 65535	21123
rat-timeout-profile	RAT timeout profile.	string	Maximum length: 63	
rate-limit-mode	GTP rate limit mode.	option	-	per-profile
	<b>Option</b> <b>Description</b>			
	<i>per-profile</i>	Per-profile rate limiting.		
	<i>per-stream</i>	Per-stream rate limiting.		
	<i>per-apn</i>	Per-APN rate limiting.		
rate-limited-log	log rate limited	option	-	disable
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
rate-sampling-interval	rate sampling interval	integer	Minimum value: 1 Maximum value: 3600	1
remove-if-echo-expires	remove if echo response expires	option	-	disable
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
remove-if-recovery-differ	remove upon different Recovery IE	option	-	disable

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
reserved-ie	reserved information element	option	-	deny
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow setting.		
	<i>deny</i>	Deny setting.		
send-delete-when-timeout	send DELETE request to path endpoints when GTPv0/v1 tunnel timeout.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
send-delete-when-timeout-v2	send DELETE request to path endpoints when GTPv2 tunnel timeout.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
spoof-src-addr	Spoofed source address for Mobile Station.	option	-	deny
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow setting.		
	<i>deny</i>	Deny setting.		
state-invalid-log	log state invalid	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
sub-second-interval	Sub-second interval.	option	-	0.5

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>0.5</td><td>Sub-second interval of 0.5 seconds.</td></tr><tr><td>0.25</td><td>Sub-second interval of 0.25 seconds.</td></tr><tr><td>0.1</td><td>Sub-second interval of 0.1 seconds.</td></tr></table>	Option	Description	0.5	Sub-second interval of 0.5 seconds.	0.25	Sub-second interval of 0.25 seconds.	0.1	Sub-second interval of 0.1 seconds.			
	Option	Description										
	0.5	Sub-second interval of 0.5 seconds.										
	0.25	Sub-second interval of 0.25 seconds.										
0.1	Sub-second interval of 0.1 seconds.											
sub-second-sampling	Enable/disable sub-second sampling.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>	Option	Description	enable	Enable setting.	disable	Disable setting.					
	Option	Description										
	enable	Enable setting.										
disable	Disable setting.											
traffic-count-log	log tunnel traffic counter	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>	Option	Description	enable	Enable setting.	disable	Disable setting.					
	Option	Description										
	enable	Enable setting.										
disable	Disable setting.											
tunnel-limit	tunnel limit	integer	Minimum value: 0 Maximum value: 4294967295	0								
tunnel-limit-log	tunnel limit	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>	Option	Description	enable	Enable setting.	disable	Disable setting.					
	Option	Description										
	enable	Enable setting.										
disable	Disable setting.											
tunnel-timeout	Established tunnel timeout (in seconds).	integer	Minimum value: 0 Maximum value: 4294967295	86400								
unknown-version-action	action for unknown gtp version	option	-	allow								

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow setting.		
	<i>deny</i>	Deny setting.		
user-plane-message-rate-limit	user plane message rate limit	integer	Minimum value: 0 Maximum value: 4294967295	0
warning-threshold	Warning threshold for rate limiting.	integer	Minimum value: 0 Maximum value: 99	0

## config apn

Parameter	Description	Type	Size	Default								
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0								
apnmember <name>	APN member. APN name.	string	Maximum length: 79									
action	Action.	option	-	allow								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow setting.</td></tr><tr><td><i>deny</i></td><td>Deny setting.</td></tr></table>				Option	Description	<i>allow</i>	Allow setting.	<i>deny</i>	Deny setting.		
Option	Description											
<i>allow</i>	Allow setting.											
<i>deny</i>	Deny setting.											
selection-mode	APN selection mode.	option	-	ms net vrf								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ms</i></td><td>Mobile Station provided APN.</td></tr><tr><td><i>net</i></td><td>Network provided APN.</td></tr><tr><td><i>vrf</i></td><td>Subscription verified.</td></tr></table>				Option	Description	<i>ms</i>	Mobile Station provided APN.	<i>net</i>	Network provided APN.	<i>vrf</i>	Subscription verified.
Option	Description											
<i>ms</i>	Mobile Station provided APN.											
<i>net</i>	Network provided APN.											
<i>vrf</i>	Subscription verified.											

## config ie-remove-policy

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
sgsn-addr	SGSN address name.	string	Maximum length: 79	all
sgsn-addr6	SGSN IPv6 address name.	string	Maximum length: 79	all
remove-ies	GTP IEs to be removed.	option	-	apn-restriction rat-type rai uli imei
		Option	Description	
		<i>apn-restriction</i>	APN Restriction.	
		<i>rat-type</i>	RAT Type.	
		<i>rai</i>	RAI.	
		<i>uli</i>	ULI.	
		<i>imei</i>	IMEI.	

## config ie-validation

Parameter	Description	Type	Size	Default
imsi	Validate IMSI.	option	-	disable
		Option	Description	
		<i>enable</i>	Enable setting.	
		<i>disable</i>	Disable setting.	
rai	Validate RAI.	option	-	disable
		Option	Description	
		<i>enable</i>	Enable setting.	
		<i>disable</i>	Disable setting.	
reordering-required	Validate re-ordering required.	option	-	disable

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
ms-validated	Validate MS validated.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
selection-mode	Validate selection mode.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
nsapi	Validate NSAPI.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
charging-ID	Validate charging ID.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
end-user-addr	Validate end user address.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
mm-context	Validate MM context.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
pdp-context	Validate PDP context.	option	-	disable



Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
gsn-addr	Validate GSN address.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
msisdn	Validate MSISDN.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
qos-profile	Validate Quality of Service(QoS) profile.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
apn-restriction	Validate APN restriction.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
rat-type	Validate RAT type.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
uli	Validate user location information.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
ms-tzone	Validate MS time zone.	option	-	disable

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
imei	Validate IMEI(SV).	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
charging-gateway-addr	Validate charging gateway address.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

## config imsi

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
mcc-mnc	MCC MNC.	string	Maximum length: 15	
msisdh-prefix	MSISDN prefix.	string	Maximum length: 15	
apnmember <name>	APN member. APN name.	string	Maximum length: 79	
action	Action.	option	-	allow
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow setting.		
	<i>deny</i>	Deny setting.		
selection-mode	APN selection mode.	option	-	ms net vrf

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>ms</i>	Mobile Station provided APN.		
	<i>net</i>	Network provided APN.		
	<i>vrf</i>	Subscription verified.		

### config ip-policy

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
srcaddr	Source address name.	string	Maximum length: 79	
dstaddr	Destination address name.	string	Maximum length: 79	
srcaddr6	Source IPv6 address name.	string	Maximum length: 79	
dstaddr6	Destination IPv6 address name.	string	Maximum length: 79	
action	Action.	option	-	allow
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow setting.		
	<i>deny</i>	Deny setting.		

### config message-rate-limit

Parameter	Description	Type	Size	Default
echo-request	Rate limit for echo requests (packets per second).	integer	Minimum value: 0 Maximum value: 4294967295	0

Parameter	Description	Type	Size	Default
echo-reponse	Rate limit for echo response (packets per second).	integer	Minimum value: 0 Maximum value: 4294967295	0
version-not-support	Rate limit for version not supported (packets per second).	integer	Minimum value: 0 Maximum value: 4294967295	0
create-pdp-request	Rate limit for create PDP context request (packets per second).	integer	Minimum value: 0 Maximum value: 4294967295	0
create-pdp-response	Rate limit for create PDP context response (packets per second).	integer	Minimum value: 0 Maximum value: 4294967295	0
update-pdp-request	Rate limit for update PDP context request (packets per second).	integer	Minimum value: 0 Maximum value: 4294967295	0
update-pdp-response	Rate limit for update PDP context response (packets per second).	integer	Minimum value: 0 Maximum value: 4294967295	0
delete-pdp-request	Rate limit for delete PDP context request (packets per second).	integer	Minimum value: 0 Maximum value: 4294967295	0
delete-pdp-response	Rate limit for delete PDP context response (packets per second).	integer	Minimum value: 0 Maximum value: 4294967295	0

Parameter	Description	Type	Size	Default
create-aa-pdp-request	Rate limit for create AA PDP context request (packets per second).	integer	Minimum value: 0 Maximum value: 4294967295	0
create-aa-pdp-response	Rate limit for create AA PDP context response (packets per second).	integer	Minimum value: 0 Maximum value: 4294967295	0
delete-aa-pdp-request	Rate limit for delete AA PDP context request (packets per second).	integer	Minimum value: 0 Maximum value: 4294967295	0
delete-aa-pdp-response	Rate limit for delete AA PDP context response (packets per second).	integer	Minimum value: 0 Maximum value: 4294967295	0
error-indication	Rate limit for error indication (packets per second).	integer	Minimum value: 0 Maximum value: 4294967295	0
pdu-notify-request	Rate limit for PDU notify request (packets per second).	integer	Minimum value: 0 Maximum value: 4294967295	0
pdu-notify-response	Rate limit for PDU notify response (packets per second).	integer	Minimum value: 0 Maximum value: 4294967295	0
pdu-notify-rej-request	Rate limit for PDU notify reject request (packets per second).	integer	Minimum value: 0 Maximum value: 4294967295	0

Parameter	Description	Type	Size	Default
pdu-notify-rej-response	Rate limit for PDU notify reject response (packets per second).	integer	Minimum value: 0 Maximum value: 4294967295	0
support-ext-hdr-notify	Rate limit for support extension headers notification (packets per second).	integer	Minimum value: 0 Maximum value: 4294967295	0
send-route-request	Rate limit for send routing information for GPRS request (packets per second).	integer	Minimum value: 0 Maximum value: 4294967295	0
send-route-response	Rate limit for send routing information for GPRS response (packets per second).	integer	Minimum value: 0 Maximum value: 4294967295	0
failure-report-request	Rate limit for failure report request (packets per second).	integer	Minimum value: 0 Maximum value: 4294967295	0
failure-report-response	Rate limit for failure report response (packets per second).	integer	Minimum value: 0 Maximum value: 4294967295	0
note-ms-request	Rate limit for note MS GPRS present request (packets per second).	integer	Minimum value: 0 Maximum value: 4294967295	0
note-ms-response	Rate limit for note MS GPRS present response (packets per second).	integer	Minimum value: 0 Maximum value: 4294967295	0

Parameter	Description	Type	Size	Default
identification-request	Rate limit for identification request (packets per second).	integer	Minimum value: 0 Maximum value: 4294967295	0
identification-response	Rate limit for identification response (packets per second).	integer	Minimum value: 0 Maximum value: 4294967295	0
sgsn-context-request	Rate limit for SGSN context request (packets per second).	integer	Minimum value: 0 Maximum value: 4294967295	0
sgsn-context-response	Rate limit for SGSN context response (packets per second).	integer	Minimum value: 0 Maximum value: 4294967295	0
sgsn-context-ack	Rate limit for SGSN context acknowledgement (packets per second).	integer	Minimum value: 0 Maximum value: 4294967295	0
fwd-relocation-request	Rate limit for forward relocation request (packets per second).	integer	Minimum value: 0 Maximum value: 4294967295	0
fwd-relocation-response	Rate limit for forward relocation response (packets per second).	integer	Minimum value: 0 Maximum value: 4294967295	0
fwd-relocation-complete	Rate limit for forward relocation complete (packets per second).	integer	Minimum value: 0 Maximum value: 4294967295	0

Parameter	Description	Type	Size	Default
relocation-cancel-request	Rate limit for relocation cancel request (packets per second).	integer	Minimum value: 0 Maximum value: 4294967295	0
relocation-cancel-response	Rate limit for relocation cancel response (packets per second).	integer	Minimum value: 0 Maximum value: 4294967295	0
fwd-srns-context	Rate limit for forward SRNS context (packets per second).	integer	Minimum value: 0 Maximum value: 4294967295	0
fwd-reloc-complete-ack	Rate limit for forward relocation complete acknowledge (packets per second).	integer	Minimum value: 0 Maximum value: 4294967295	0
fwd-srns-context-ack	Rate limit for forward SRNS context acknowledge (packets per second).	integer	Minimum value: 0 Maximum value: 4294967295	0
ran-info	Rate limit for RAN information relay (packets per second).	integer	Minimum value: 0 Maximum value: 4294967295	0
mbms-notify-request	Rate limit for MBMS notification request (packets per second).	integer	Minimum value: 0 Maximum value: 4294967295	0
mbms-notify-response	Rate limit for MBMS notification response (packets per second).	integer	Minimum value: 0 Maximum value: 4294967295	0



Parameter	Description	Type	Size	Default
mbms-notify-rej-request	Rate limit for MBMS notification reject request (packets per second).	integer	Minimum value: 0 Maximum value: 4294967295	0
mbms-notify-rej-response	Rate limit for MBMS notification reject response (packets per second).	integer	Minimum value: 0 Maximum value: 4294967295	0
create-mbms-request	Rate limit for create MBMS context request (packets per second).	integer	Minimum value: 0 Maximum value: 4294967295	0
create-mbms-response	Rate limit for create MBMS context response (packets per second).	integer	Minimum value: 0 Maximum value: 4294967295	0
update-mbms-request	Rate limit for update MBMS context request (packets per second).	integer	Minimum value: 0 Maximum value: 4294967295	0
update-mbms-response	Rate limit for update MBMS context response (packets per second).	integer	Minimum value: 0 Maximum value: 4294967295	0
delete-mbms-request	Rate limit for delete MBMS context request (packets per second).	integer	Minimum value: 0 Maximum value: 4294967295	0
delete-mbms-response	Rate limit for delete MBMS context response (packets per second).	integer	Minimum value: 0 Maximum value: 4294967295	0

Parameter	Description	Type	Size	Default
mbms-reg-request	Rate limit for MBMS registration request (packets per second).	integer	Minimum value: 0 Maximum value: 4294967295	0
mbms-reg-response	Rate limit for MBMS registration response (packets per second).	integer	Minimum value: 0 Maximum value: 4294967295	0
mbms-de-reg-request	Rate limit for MBMS de-registration request (packets per second).	integer	Minimum value: 0 Maximum value: 4294967295	0
mbms-de-reg-response	Rate limit for MBMS de-registration response (packets per second).	integer	Minimum value: 0 Maximum value: 4294967295	0
mbms-ses-start-request	Rate limit for MBMS session start request (packets per second).	integer	Minimum value: 0 Maximum value: 4294967295	0
mbms-ses-start-response	Rate limit for MBMS session start response (packets per second).	integer	Minimum value: 0 Maximum value: 4294967295	0
mbms-ses-stop-request	Rate limit for MBMS session stop request (packets per second).	integer	Minimum value: 0 Maximum value: 4294967295	0
mbms-ses-stop-response	Rate limit for MBMS session stop response (packets per second).	integer	Minimum value: 0 Maximum value: 4294967295	0

Parameter	Description	Type	Size	Default
g-pdu	Rate limit for G-PDU (packets per second).	integer	Minimum value: 0 Maximum value: 4294967295	0

#### config message-rate-limit-v0

Parameter	Description	Type	Size	Default
echo-request	Rate limit (packets/s) for echo request.	integer	Minimum value: 0 Maximum value: 4294967295	0
create-pdp-request	Rate limit (packets/s) for create PDP context request.	integer	Minimum value: 0 Maximum value: 4294967295	0
delete-pdp-request	Rate limit (packets/s) for delete PDP context request.	integer	Minimum value: 0 Maximum value: 4294967295	0

#### config message-rate-limit-v1

Parameter	Description	Type	Size	Default
echo-request	Rate limit (packets/s) for echo request.	integer	Minimum value: 0 Maximum value: 4294967295	0
create-pdp-request	Rate limit (packets/s) for create PDP context request.	integer	Minimum value: 0 Maximum value: 4294967295	0
delete-pdp-request	Rate limit (packets/s) for delete PDP context request.	integer	Minimum value: 0 Maximum value: 4294967295	0

## config message-rate-limit-v2

Parameter	Description	Type	Size	Default
echo-request	Rate limit (packets/s) for echo request.	integer	Minimum value: 0 Maximum value: 4294967295	0
create-session-request	Rate limit (packets/s) for create session request.	integer	Minimum value: 0 Maximum value: 4294967295	0
delete-session-request	Rate limit (packets/s) for delete session request.	integer	Minimum value: 0 Maximum value: 4294967295	0

## config noip-policy

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
type	Protocol field type.	option	-	etsi
	Option	Description		
	etsi	ESTI.		
	ietf	IETF.		
start	Start of protocol range.	integer	Minimum value: 0 Maximum value: 255	0
end	End of protocol range.	integer	Minimum value: 0 Maximum value: 255	0
action	Action.	option	-	allow

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow setting.		
	<i>deny</i>	Deny setting.		

### config per-apn-shaper

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
apn	APN name.	string	Maximum length: 63	
version	GTP version number: 0 or 1.	integer	Minimum value: 0 Maximum value: 1	1
rate-limit	Rate limit (packets/s) for create PDP context request.	integer	Minimum value: 0 Maximum value: 1000000	0

### config policy

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
apnmember <name>	APN member. APN name.	string	Maximum length: 79	
messages	GTP messages.	option	-	create-req
	<b>Option</b>	<b>Description</b>		
	<i>create-req</i>	Create PDP context request.		

Parameter	Description	Type	Size	Default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>create-res</i></td><td>Create PDP context response.</td></tr><tr><td><i>update-req</i></td><td>Update PDP context request.</td></tr><tr><td><i>update-res</i></td><td>Update PDP context response.</td></tr></table>	Option	Description	<i>create-res</i>	Create PDP context response.	<i>update-req</i>	Update PDP context request.	<i>update-res</i>	Update PDP context response.									
	Option	Description																
	<i>create-res</i>	Create PDP context response.																
	<i>update-req</i>	Update PDP context request.																
<i>update-res</i>	Update PDP context response.																	
apn-sel-mode	APN selection mode.	option	-	ms net vrf														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ms</i></td><td>Mobile Station provided APN.</td></tr><tr><td><i>net</i></td><td>Network provided APN.</td></tr><tr><td><i>vrf</i></td><td>Subscription verified.</td></tr></table>	Option	Description	<i>ms</i>	Mobile Station provided APN.	<i>net</i>	Network provided APN.	<i>vrf</i>	Subscription verified.									
	Option	Description																
	<i>ms</i>	Mobile Station provided APN.																
	<i>net</i>	Network provided APN.																
<i>vrf</i>	Subscription verified.																	
max-apn-restriction	Maximum APN restriction value.	option	-	all														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>all</i></td><td>All.</td></tr><tr><td><i>public-1</i></td><td>Public-1.</td></tr><tr><td><i>public-2</i></td><td>Public-2.</td></tr><tr><td><i>private-1</i></td><td>Private-1.</td></tr><tr><td><i>private-2</i></td><td>Private-2.</td></tr></table>	Option	Description	<i>all</i>	All.	<i>public-1</i>	Public-1.	<i>public-2</i>	Public-2.	<i>private-1</i>	Private-1.	<i>private-2</i>	Private-2.					
	Option	Description																
	<i>all</i>	All.																
	<i>public-1</i>	Public-1.																
	<i>public-2</i>	Public-2.																
	<i>private-1</i>	Private-1.																
<i>private-2</i>	Private-2.																	
imsi-prefix	IMSI prefix.	string	Maximum length: 15															
msisdn-prefix	MSISDN prefix.	string	Maximum length: 15															
rat-type	RAT Type.	option	-	any														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>any</i></td><td>Any RAT.</td></tr><tr><td><i>utran</i></td><td>UTRAN.</td></tr><tr><td><i>geran</i></td><td>GERAN.</td></tr><tr><td><i>wlan</i></td><td>WLAN.</td></tr><tr><td><i>gan</i></td><td>GAN.</td></tr><tr><td><i>hspa</i></td><td>HSPA.</td></tr></table>	Option	Description	<i>any</i>	Any RAT.	<i>utran</i>	UTRAN.	<i>geran</i>	GERAN.	<i>wlan</i>	WLAN.	<i>gan</i>	GAN.	<i>hspa</i>	HSPA.			
	Option	Description																
	<i>any</i>	Any RAT.																
	<i>utran</i>	UTRAN.																
	<i>geran</i>	GERAN.																
	<i>wlan</i>	WLAN.																
	<i>gan</i>	GAN.																
<i>hspa</i>	HSPA.																	

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>eutran</i>	EUTRAN.		
	<i>virtual</i>	Virtual.		
	<i>nbiot</i>	NB-IoT.		
imei	IMEI pattern.	string	Maximum length: 40	
action	Action.	option	-	allow
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow setting.		
	<i>deny</i>	Deny setting.		
rai	RAI pattern.	string	Maximum length: 40	
uli	ULI pattern.	string	Maximum length: 40	

## config policy-v2

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
apnmember <name>	APN member. APN name.	string	Maximum length: 79	
messages	GTP messages.	option	-	create-ses-req
	<b>Option</b>	<b>Description</b>		
	<i>create-ses-req</i>	Create session request.		
	<i>create-ses-res</i>	Create session response.		
	<i>modify-bearer-req</i>	Modify bearer request.		
	<i>modify-bearer-res</i>	Modify bearer response.		

Parameter	Description	Type	Size	Default
apn-sel-mode	APN selection mode.	option	-	ms net vrf
	<b>Option</b>	<b>Description</b>		
	<i>ms</i>	Mobile Station provided APN.		
	<i>net</i>	Network provided APN.		
	<i>vrf</i>	Subscription verified.		
max-apn-restriction	Maximum APN restriction value.	option	-	all
	<b>Option</b>	<b>Description</b>		
	<i>all</i>	All.		
	<i>public-1</i>	Public-1.		
	<i>public-2</i>	Public-2.		
	<i>private-1</i>	Private-1.		
	<i>private-2</i>	Private-2.		
imsi-prefix	IMSI prefix.	string	Maximum length: 15	
msisdn-prefix	MSISDN prefix.	string	Maximum length: 15	
rat-type	RAT Type.	option	-	any
	<b>Option</b>	<b>Description</b>		
	<i>any</i>	Any RAT.		
	<i>utran</i>	UTRAN.		
	<i>geran</i>	GERAN.		
	<i>wlan</i>	WLAN.		
	<i>gan</i>	GAN.		
	<i>hspa</i>	HSPA.		
	<i>eutran</i>	EUTRAN.		
	<i>virtual</i>	Virtual.		
	<i>nbiot</i>	NB-IoT.		
	<i>ltem</i>	LTE-M.		
	<i>nr</i>	NR.		



Parameter	Description	Type	Size	Default						
mei	MEI pattern.	string	Maximum length: 40							
action	Action.	option	-	allow						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow setting.</td></tr><tr><td><i>deny</i></td><td>Deny setting.</td></tr></table>				Option	Description	<i>allow</i>	Allow setting.	<i>deny</i>	Deny setting.
	Option	Description								
	<i>allow</i>	Allow setting.								
<i>deny</i>	Deny setting.									
uli	GTPv2 ULI patterns (in order of CGI SAI RAI TAI ECGI LAI).	string	Maximum length: 40							

## config firewall identity-based-route

Configure identity based routing.

```
config firewall identity-based-route
    Description: Configure identity based routing.
    edit <name>
        set comments {string}
        config rule
            Description: Rule.
            edit <id>
                set gateway {ipv4-address}
                set device {string}
                set groups <name1>, <name2>, ...
            next
        end
    next
end
```

## config firewall identity-based-route

Parameter	Description	Type	Size	Default
comments	Comments.	string	Maximum length: 127	
name	Name.	string	Maximum length: 35	

## config rule

Parameter	Description	Type	Size	Default
id	Rule ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
gateway	IPv4 address of the gateway (Format: xxx.xxx.xxx.xxx, Default: 0.0.0.0).	ipv4-address	Not Specified	0.0.0.0
device	Outgoing interface for the rule.	string	Maximum length: 35	
groups <name>	Select one or more group(s) from available groups that are allowed to use this route. Separate group names with a space. Group name.	string	Maximum length: 79	

## config firewall interface-policy

Configure IPv4 interface policies.

```
config firewall interface-policy
  Description: Configure IPv4 interface policies.
  edit <policyid>
    set application-list {string}
    set application-list-status [enable|disable]
    set av-profile {string}
    set av-profile-status [enable|disable]
    set comments {var-string}
    set dlp-sensor {string}
    set dlp-sensor-status [enable|disable]
    set dsri [enable|disable]
    set dstaddr <name1>, <name2>, ...
    set emailfilter-profile {string}
    set emailfilter-profile-status [enable|disable]
    set interface {string}
    set ips-sensor {string}
    set ips-sensor-status [enable|disable]
    set logtraffic [all|utm|...]
    set service <name1>, <name2>, ...
    set srcaddr <name1>, <name2>, ...
    set status [enable|disable]
    set webfilter-profile {string}
    set webfilter-profile-status [enable|disable]
  next
end
```

## config firewall interface-policy

Parameter	Description	Type	Size	Default						
application-list	Application list name.	string	Maximum length: 35							
application-list-status	Enable/disable application control.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable application control</td></tr><tr><td><i>disable</i></td><td>Disable application control</td></tr></table>	Option	Description	<i>enable</i>	Enable application control	<i>disable</i>	Disable application control			
Option	Description									
<i>enable</i>	Enable application control									
<i>disable</i>	Disable application control									
av-profile	Antivirus profile.	string	Maximum length: 35							
av-profile-status	Enable/disable antivirus.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable antivirus</td></tr><tr><td><i>disable</i></td><td>Disable antivirus</td></tr></table>	Option	Description	<i>enable</i>	Enable antivirus	<i>disable</i>	Disable antivirus			
Option	Description									
<i>enable</i>	Enable antivirus									
<i>disable</i>	Disable antivirus									
comments	Comments.	var-string	Maximum length: 1023							
dlp-sensor	DLP sensor name.	string	Maximum length: 35							
dlp-sensor-status	Enable/disable DLP.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
dsri	Enable/disable DSRI.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable DSRI.</td></tr><tr><td><i>disable</i></td><td>Disable DSRI.</td></tr></table>	Option	Description	<i>enable</i>	Enable DSRI.	<i>disable</i>	Disable DSRI.			
Option	Description									
<i>enable</i>	Enable DSRI.									
<i>disable</i>	Disable DSRI.									
dstaddr <name>	Address object to limit traffic monitoring to network traffic sent to the specified address or range. Address name.	string	Maximum length: 79							

Parameter	Description	Type	Size	Default								
emailfilter-profile	Email filter profile.	string	Maximum length: 35									
emailfilter-profile-status	Enable/disable email filter.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Email filter.</td></tr><tr><td><i>disable</i></td><td>Disable Email filter.</td></tr></table>	Option	Description	<i>enable</i>	Enable Email filter.	<i>disable</i>	Disable Email filter.					
Option	Description											
<i>enable</i>	Enable Email filter.											
<i>disable</i>	Disable Email filter.											
interface	Monitored interface name from available interfaces.	string	Maximum length: 35									
ips-sensor	IPS sensor name.	string	Maximum length: 35									
ips-sensor-status	Enable/disable IPS.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable IPS.</td></tr><tr><td><i>disable</i></td><td>Disable IPS.</td></tr></table>	Option	Description	<i>enable</i>	Enable IPS.	<i>disable</i>	Disable IPS.					
Option	Description											
<i>enable</i>	Enable IPS.											
<i>disable</i>	Disable IPS.											
logtraffic	Logging type to be used in this policy (Options: all   utm   disable, Default: utm).	option	-	utm								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>all</i></td><td>Log all sessions accepted or denied by this policy.</td></tr><tr><td><i>utm</i></td><td>Log traffic that has a security profile applied to it.</td></tr><tr><td><i>disable</i></td><td>Disable all logging for this policy.</td></tr></table>	Option	Description	<i>all</i>	Log all sessions accepted or denied by this policy.	<i>utm</i>	Log traffic that has a security profile applied to it.	<i>disable</i>	Disable all logging for this policy.			
Option	Description											
<i>all</i>	Log all sessions accepted or denied by this policy.											
<i>utm</i>	Log traffic that has a security profile applied to it.											
<i>disable</i>	Disable all logging for this policy.											
policyid	Policy ID.	integer	Minimum value: 0 Maximum value: 4294967295	0								
service <name>	Service object from available options. Service name.	string	Maximum length: 79									
srcaddr <name>	Address object to limit traffic monitoring to network traffic sent from the specified address or range. Address name.	string	Maximum length: 79									
status	Enable/disable this policy.	option	-	enable								

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable this policy.		
	<i>disable</i>	Disable this policy.		
webfilter-profile	Web filter profile.	string	Maximum length: 35	
webfilter-profile-status	Enable/disable web filtering.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable web filtering.		
	<i>disable</i>	Disable web filtering.		

## config firewall interface-policy6

Configure IPv6 interface policies.

```
config firewall interface-policy6
    Description: Configure IPv6 interface policies.
    edit <policyid>
        set application-list {string}
        set application-list-status [enable|disable]
        set av-profile {string}
        set av-profile-status [enable|disable]
        set comments {var-string}
        set dlp-sensor {string}
        set dlp-sensor-status [enable|disable]
        set dsri [enable|disable]
        set dstaddr6 <name1>, <name2>, ...
        set emailfilter-profile {string}
        set emailfilter-profile-status [enable|disable]
        set interface {string}
        set ips-sensor {string}
        set ips-sensor-status [enable|disable]
        set logtraffic [all|utm|...]
        set service6 <name1>, <name2>, ...
        set srcaddr6 <name1>, <name2>, ...
        set status [enable|disable]
        set webfilter-profile {string}
        set webfilter-profile-status [enable|disable]
    next
end
```

## config firewall interface-policy6

Parameter	Description	Type	Size	Default						
application-list	Application list name.	string	Maximum length: 35							
application-list-status	Enable/disable application control.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable application control</td></tr><tr><td><i>disable</i></td><td>Disable application control</td></tr></table>	Option	Description	<i>enable</i>	Enable application control	<i>disable</i>	Disable application control			
Option	Description									
<i>enable</i>	Enable application control									
<i>disable</i>	Disable application control									
av-profile	Antivirus profile.	string	Maximum length: 35							
av-profile-status	Enable/disable antivirus.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable antivirus</td></tr><tr><td><i>disable</i></td><td>Disable antivirus</td></tr></table>	Option	Description	<i>enable</i>	Enable antivirus	<i>disable</i>	Disable antivirus			
Option	Description									
<i>enable</i>	Enable antivirus									
<i>disable</i>	Disable antivirus									
comments	Comments.	var-string	Maximum length: 1023							
dlp-sensor	DLP sensor name.	string	Maximum length: 35							
dlp-sensor-status	Enable/disable DLP.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
dsri	Enable/disable DSRI.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable DSRI.</td></tr><tr><td><i>disable</i></td><td>Disable DSRI.</td></tr></table>	Option	Description	<i>enable</i>	Enable DSRI.	<i>disable</i>	Disable DSRI.			
Option	Description									
<i>enable</i>	Enable DSRI.									
<i>disable</i>	Disable DSRI.									
dstaddr6 <name>	IPv6 address object to limit traffic monitoring to network traffic sent to the specified address or range. Address name.	string	Maximum length: 79							

Parameter	Description	Type	Size	Default								
emailfilter-profile	Email filter profile.	string	Maximum length: 35									
emailfilter-profile-status	Enable/disable email filter.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Email filter.</td></tr><tr><td><i>disable</i></td><td>Disable Email filter.</td></tr></table>	Option	Description	<i>enable</i>	Enable Email filter.	<i>disable</i>	Disable Email filter.					
Option	Description											
<i>enable</i>	Enable Email filter.											
<i>disable</i>	Disable Email filter.											
interface	Monitored interface name from available interfaces.	string	Maximum length: 35									
ips-sensor	IPS sensor name.	string	Maximum length: 35									
ips-sensor-status	Enable/disable IPS.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable IPS.</td></tr><tr><td><i>disable</i></td><td>Disable IPS.</td></tr></table>	Option	Description	<i>enable</i>	Enable IPS.	<i>disable</i>	Disable IPS.					
Option	Description											
<i>enable</i>	Enable IPS.											
<i>disable</i>	Disable IPS.											
logtraffic	Logging type to be used in this policy (Options: all   utm   disable, Default: utm).	option	-	utm								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>all</i></td><td>Log all sessions accepted or denied by this policy.</td></tr><tr><td><i>utm</i></td><td>Log traffic that has a security profile applied to it.</td></tr><tr><td><i>disable</i></td><td>Disable all logging for this policy.</td></tr></table>	Option	Description	<i>all</i>	Log all sessions accepted or denied by this policy.	<i>utm</i>	Log traffic that has a security profile applied to it.	<i>disable</i>	Disable all logging for this policy.			
Option	Description											
<i>all</i>	Log all sessions accepted or denied by this policy.											
<i>utm</i>	Log traffic that has a security profile applied to it.											
<i>disable</i>	Disable all logging for this policy.											
policyid	Policy ID.	integer	Minimum value: 0 Maximum value: 4294967295	0								
service6 <name>	Service name. Address name.	string	Maximum length: 79									
srcaddr6 <name>	IPv6 address object to limit traffic monitoring to network traffic sent from the specified address or range. Address name.	string	Maximum length: 79									
status	Enable/disable this policy.	option	-	enable								

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable this policy.		
	<i>disable</i>	Disable this policy.		
webfilter-profile	Web filter profile.	string	Maximum length: 35	
webfilter-profile-status	Enable/disable web filtering.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable web filtering.		
	<i>disable</i>	Disable web filtering.		

## config firewall internet-service-addition

Configure Internet Services Addition.

```
config firewall internet-service-addition
  Description: Configure Internet Services Addition.
  edit <id>
    set comment {var-string}
    config entry
      Description: Entries added to the Internet Service addition database.
      edit <id>
        set protocol {integer}
        config port-range
          Description: Port ranges in the custom entry.
          edit <id>
            set start-port {integer}
            set end-port {integer}
          next
        next
      end
    next
  end
end
```

## config firewall internet-service-addition

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 255	



Parameter	Description	Type	Size	Default
id	Internet Service ID in the Internet Service database.	integer	Minimum value: 0 Maximum value: 4294967295	0

### config entry

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 255	0
protocol	Integer value for the protocol type as defined by IANA.	integer	Minimum value: 0 Maximum value: 255	0

### config port-range

Parameter	Description	Type	Size	Default
id	Custom entry port range ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
start-port	Integer value for starting TCP/UDP/SCTP destination port in range (0 to 65535).	integer	Minimum value: 0 Maximum value: 65535	1
end-port	Integer value for ending TCP/UDP/SCTP destination port in range (0 to 65535).	integer	Minimum value: 0 Maximum value: 65535	65535

## config firewall internet-service-append

Configure additional port mappings for Internet Services.

```
config firewall internet-service-append
    Description: Configure additional port mappings for Internet Services.
    set append-port {integer}
    set match-port {integer}
end
```

## config firewall internet-service-append

Parameter	Description	Type	Size	Default
append-port	Appending TCP/UDP/SCTP destination port (1 to 65535).	integer	Minimum value: 1 Maximum value: 65535	0
match-port	Matching TCP/UDP/SCTP destination port (0 to 65535, 0 means any port).	integer	Minimum value: 0 Maximum value: 65535	0

## config firewall internet-service-botnet

Show Internet Service botnet.

```
config firewall internet-service-botnet
    Description: Show Internet Service botnet.
    edit <id>
        set name {string}
    next
end
```

## config firewall internet-service-botnet

Parameter	Description	Type	Size	Default
id	Internet Service Botnet ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
name	Internet Service Botnet name.	string	Maximum length: 63	

## config firewall internet-service-custom-group

Configure custom Internet Service group.

```
config firewall internet-service-custom-group
    Description: Configure custom Internet Service group.
    edit <name>
        set comment {var-string}
        set member <name1>, <name2>, ...
    next
end
```

```
    next
end
```

## config firewall internet-service-custom-group

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 255	
member <name>	Custom Internet Service group members. Group member name.	string	Maximum length: 79	
name	Custom Internet Service group name.	string	Maximum length: 63	

## config firewall internet-service-custom

Configure custom Internet Services.

```
config firewall internet-service-custom
  Description: Configure custom Internet Services.
  edit <name>
    set comment {var-string}
    config entry
      Description: Entries added to the Internet Service database and custom database.
      edit <id>
        set protocol {integer}
        config port-range
          Description: Port ranges in the custom entry.
          edit <id>
            set start-port {integer}
            set end-port {integer}
          next
        end
        set dst <name1>, <name2>, ...
      next
    end
    set reputation {integer}
  next
end
```

## config firewall internet-service-custom

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 255	
name	Internet Service name.	string	Maximum length: 63	

Parameter	Description	Type	Size	Default
reputation	Reputation level of the custom Internet Service.	integer	Minimum value: 0 Maximum value: 4294967295	3

### config entry

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 255	0
protocol	Integer value for the protocol type as defined by IANA.	integer	Minimum value: 0 Maximum value: 255	0
dst <name>	Destination address or address group name. Select the destination address or address group object from available options.	string	Maximum length: 79	

### config port-range

Parameter	Description	Type	Size	Default
id	Custom entry port range ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
start-port	Integer value for starting TCP/UDP/SCTP destination port in range (0 to 65535).	integer	Minimum value: 0 Maximum value: 65535	1
end-port	Integer value for ending TCP/UDP/SCTP destination port in range (0 to 65535).	integer	Minimum value: 0 Maximum value: 65535	65535

## config firewall internet-service-definition

Configure Internet Service definition.

```

config firewall internet-service-definition
  Description: Configure Internet Service definition.
  edit <id>
    config entry
      Description: Protocol and port information in an Internet Service entry.
      edit <seq-num>
        set category-id {integer}
        set name {string}
        set protocol {integer}
        config port-range
          Description: Port ranges in the definition entry.
          edit <id>
            set start-port {integer}
            set end-port {integer}
          next
        end
      next
    end
  next
end

```

## config firewall internet-service-definition

Parameter	Description	Type	Size	Default
id	Internet Service application list ID.	integer	Minimum value: 0 Maximum value: 4294967295	0

## config entry

Parameter	Description	Type	Size	Default
seq-num	Entry sequence number.	integer	Minimum value: 0 Maximum value: 4294967295	7 **
category-id	Internet Service category ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
name	Internet Service name.	string	Maximum length: 63	

Parameter	Description	Type	Size	Default
protocol	Integer value for the protocol type as defined by IANA.	integer	Minimum value: 0 Maximum value: 255	0

\*\* Values may differ between models.

### config port-range

Parameter	Description	Type	Size	Default
id	Custom entry port range ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
start-port	Starting TCP/UDP/SCTP destination port (1 to 65535).	integer	Minimum value: 1 Maximum value: 65535	1
end-port	Ending TCP/UDP/SCTP destination port (1 to 65535).	integer	Minimum value: 1 Maximum value: 65535	65535

## config firewall internet-service-extension

Configure Internet Services Extension.

```
config firewall internet-service-extension
  Description: Configure Internet Services Extension.
  edit <id>
    set comment {var-string}
    config disable-entry
      Description: Disable entries in the Internet Service database.
      edit <id>
        set protocol {integer}
        config port-range
          Description: Port ranges in the disable entry.
          edit <id>
            set start-port {integer}
            set end-port {integer}
          next
        end
      config ip-range
        Description: IP ranges in the disable entry.
        edit <id>
          set start-ip {ipv4-address-any}
```

```

        set end-ip {ipv4-address-any}
    next
end
next
end
config entry
    Description: Entries added to the Internet Service extension database.
    edit <id>
        set protocol {integer}
        config port-range
            Description: Port ranges in the custom entry.
            edit <id>
                set start-port {integer}
                set end-port {integer}
            next
        end
        set dst <name1>, <name2>, ...
    next
end
next
end

```

## config firewall internet-service-extension

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 255	
id	Internet Service ID in the Internet Service database.	integer	Minimum value: 0 Maximum value: 4294967295	0

## config disable-entry

Parameter	Description	Type	Size	Default
id	Disable entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
protocol	Integer value for the protocol type as defined by IANA.	integer	Minimum value: 0 Maximum value: 255	0

### config port-range

Parameter	Description	Type	Size	Default
id	Custom entry port range ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
start-port	Integer value for starting TCP/UDP/SCTP destination port in range (0 to 65535).	integer	Minimum value: 0 Maximum value: 65535	1
end-port	Integer value for ending TCP/UDP/SCTP destination port in range (0 to 65535).	integer	Minimum value: 0 Maximum value: 65535	65535

### config ip-range

Parameter	Description	Type	Size	Default
id	Disable entry range ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
start-ip	Start IP address.	ipv4-address-any	Not Specified	0.0.0.0
end-ip	End IP address.	ipv4-address-any	Not Specified	0.0.0.0

### config entry

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 255	0
protocol	Integer value for the protocol type as defined by IANA.	integer	Minimum value: 0 Maximum value: 255	0



Parameter	Description	Type	Size	Default
dst <name>	Destination address or address group name. Select the destination address or address group object from available options.	string	Maximum length: 79	

### config port-range

Parameter	Description	Type	Size	Default
id	Custom entry port range ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
start-port	Integer value for starting TCP/UDP/SCTP destination port in range (0 to 65535).	integer	Minimum value: 0 Maximum value: 65535	1
end-port	Integer value for ending TCP/UDP/SCTP destination port in range (0 to 65535).	integer	Minimum value: 0 Maximum value: 65535	65535

## config firewall internet-service-group

Configure group of Internet Service.

```
config firewall internet-service-group
    Description: Configure group of Internet Service.
    edit <name>
        set comment {var-string}
        set direction [source|destination|...]
        set member <name1>, <name2>, ...
    next
end
```

### config firewall internet-service-group

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 255	
direction	How this service may be used (source, destination or both).	option	-	both

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>source</i>	As source when applied.		
	<i>destination</i>	As destination when applied.		
	<i>both</i>	Both directions when applied.		
member <name>	Internet Service group member. Internet Service name.	string	Maximum length: 79	
name	Internet Service group name.	string	Maximum length: 63	

## config firewall internet-service-ipbl-reason

IP block list reason.

```
config firewall internet-service-ipbl-reason
    Description: IP block list reason.
    edit <id>
        set name {string}
    next
end
```

## config firewall internet-service-ipbl-reason

Parameter	Description	Type	Size	Default
id	IP block list reason ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
name	IP block list reason name.	string	Maximum length: 63	

## config firewall internet-service-ipbl-vendor

IP block list vendor.

```
config firewall internet-service-ipbl-vendor
    Description: IP block list vendor.
    edit <id>
        set name {string}
    next
end
```

## config firewall internet-service-ipbl-vendor

Parameter	Description	Type	Size	Default
id	IP block list vendor ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
name	IP block list vendor name.	string	Maximum length: 63	

## config firewall internet-service-list

Internet Service list.

```
config firewall internet-service-list
  Description: Internet Service list.
  edit <id>
    set name {string}
  next
end
```

## config firewall internet-service-list

Parameter	Description	Type	Size	Default
id	Internet Service category ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
name	Internet Service category name.	string	Maximum length: 63	

## config firewall internet-service-name

Define internet service names.

```
config firewall internet-service-name
  Description: Define internet service names.
  edit <name>
    set city-id {integer}
    set country-id {integer}
    set internet-service-id {integer}
    set region-id {integer}
    set type [default|location]
```

```
next
end
```

## config firewall internet-service-name

Parameter	Description	Type	Size	Default
city-id	City ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
country-id	Country or Area ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
internet-service-id	Internet Service ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
name	Internet Service name.	string	Maximum length: 63	
region-id	Region ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
type	Internet Service name type.	option	-	default
	Option	Description		
	default	Automatically generated Internet Service.		
	location	Geography location based Internet Service.		

## config firewall internet-service-owner

Internet Service owner.

```
config firewall internet-service-owner
  Description: Internet Service owner.
  edit <id>
    set name {string}
  next
end
```

## config firewall internet-service-owner

Parameter	Description	Type	Size	Default
id	Internet Service owner ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
name	Internet Service owner name.	string	Maximum length: 63	

## config firewall internet-service-reputation

Show Internet Service reputation.

```
config firewall internet-service-reputation
  Description: Show Internet Service reputation.
  edit <id>
    set description {string}
  next
end
```

## config firewall internet-service-reputation

Parameter	Description	Type	Size	Default
description	Description.	string	Maximum length: 127	
id	Internet Service Reputation ID.	integer	Minimum value: 0 Maximum value: 4294967295	0

## config firewall internet-service-sld

Internet Service Second Level Domain.

```
config firewall internet-service-sld
  Description: Internet Service Second Level Domain.
  edit <id>
    set name {string}
  next
end
```

## config firewall internet-service-sld

Parameter	Description	Type	Size	Default
id	Second Level Domain ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
name	Second Level Domain name.	string	Maximum length: 63	

## config firewall internet-service

Show Internet Service application.

```
config firewall internet-service
  Description: Show Internet Service application.
  edit <id>
    set database [isdb|irdb]
    set direction [src|dst|...]
    set extra-ip-range-number {integer}
    set icon-id {integer}
    set ip-number {integer}
    set ip-range-number {integer}
    set name {string}
    set obsolete {integer}
    set singularity {integer}
  next
end
```

## config firewall internet-service

Parameter	Description	Type	Size	Default						
database	Database name this Internet Service belongs to.	option	-	isdb						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>isdb</i></td><td>Internet Service Database.</td></tr><tr><td><i>irdb</i></td><td>Internet RRR Database.</td></tr></table>	Option	Description	<i>isdb</i>	Internet Service Database.	<i>irdb</i>	Internet RRR Database.			
Option	Description									
<i>isdb</i>	Internet Service Database.									
<i>irdb</i>	Internet RRR Database.									
direction	How this service may be used in a firewall policy (source, destination or both).	option	-	both						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>src</i></td><td>As source in the firewall policy.</td></tr></table>	Option	Description	<i>src</i>	As source in the firewall policy.					
Option	Description									
<i>src</i>	As source in the firewall policy.									

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>dst</i></td><td>As destination in the firewall policy.</td></tr><tr><td><i>both</i></td><td>Both directions in the firewall policy.</td></tr></table>	Option	Description	<i>dst</i>	As destination in the firewall policy.	<i>both</i>	Both directions in the firewall policy.			
	Option	Description								
	<i>dst</i>	As destination in the firewall policy.								
<i>both</i>	Both directions in the firewall policy.									
extra-ip-range-number	Extra number of IP ranges.	integer	Minimum value: 0 Maximum value: 4294967295	0						
icon-id	Icon ID of Internet Service.	integer	Minimum value: 0 Maximum value: 4294967295	0						
id	Internet Service ID.	integer	Minimum value: 0 Maximum value: 4294967295	0						
ip-number	Total number of IP addresses.	integer	Minimum value: 0 Maximum value: 4294967295	0						
ip-range-number	Number of IP ranges.	integer	Minimum value: 0 Maximum value: 4294967295	0						
name	Internet Service name.	string	Maximum length: 63							
obsolete	Indicates whether the Internet Service can be used.	integer	Minimum value: 0 Maximum value: 255	0						
singularity	Singular level of the Internet Service.	integer	Minimum value: 0 Maximum value: 65535	0						

## config firewall ip-translation

Configure firewall IP-translation.

```
config firewall ip-translation
  Description: Configure firewall IP-translation.
  edit <transid>
    set endip {ipv4-address-any}
    set map-startip {ipv4-address-any}
    set startip {ipv4-address-any}
    set type {option}
  next
end
```

## config firewall ip-translation

Parameter	Description	Type	Size	Default
endip	Final IPv4 address.	ipv4-address-any	Not Specified	0.0.0.0
map-startip	Address to be used as the starting point for translation in the range.	ipv4-address-any	Not Specified	0.0.0.0
startip	First IPv4 address.	ipv4-address-any	Not Specified	0.0.0.0
transid	IP translation ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
type	IP translation type (option: SCTP).	option	-	SCTP
		Option	Description	
		SCTP	SCTP	

## config firewall ipmacbinding setting

Configure IP to MAC binding settings.

```
config firewall ipmacbinding setting
  Description: Configure IP to MAC binding settings.
  set bindthroughfw [enable|disable]
  set bindtofw [enable|disable]
  set undefinedhost [allow|block]
end
```



## config firewall ipmacbinding setting

Parameter	Description	Type	Size	Default						
bindthroughfw	Enable/disable use of IP/MAC binding to filter packets that would normally go through the firewall.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable IP/MAC binding for packets that would normally go through the firewall.</td></tr><tr><td><i>disable</i></td><td>Disable IP/MAC binding for packets that would normally go through the firewall.</td></tr></table>	Option	Description	<i>enable</i>	Enable IP/MAC binding for packets that would normally go through the firewall.	<i>disable</i>	Disable IP/MAC binding for packets that would normally go through the firewall.			
Option	Description									
<i>enable</i>	Enable IP/MAC binding for packets that would normally go through the firewall.									
<i>disable</i>	Disable IP/MAC binding for packets that would normally go through the firewall.									
bindtofw	Enable/disable use of IP/MAC binding to filter packets that would normally go to the firewall.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable IP/MAC binding for packets that would normally go to the firewall.</td></tr><tr><td><i>disable</i></td><td>Disable IP/MAC binding for packets that would normally go to the firewall.</td></tr></table>	Option	Description	<i>enable</i>	Enable IP/MAC binding for packets that would normally go to the firewall.	<i>disable</i>	Disable IP/MAC binding for packets that would normally go to the firewall.			
Option	Description									
<i>enable</i>	Enable IP/MAC binding for packets that would normally go to the firewall.									
<i>disable</i>	Disable IP/MAC binding for packets that would normally go to the firewall.									
undefinedhost	Select action to take on packets with IP/MAC addresses not in the binding list.	option	-	block						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow packets from MAC addresses not in the IP/MAC list.</td></tr><tr><td><i>block</i></td><td>Block packets from MAC addresses not in the IP/MAC list.</td></tr></table>	Option	Description	<i>allow</i>	Allow packets from MAC addresses not in the IP/MAC list.	<i>block</i>	Block packets from MAC addresses not in the IP/MAC list.			
Option	Description									
<i>allow</i>	Allow packets from MAC addresses not in the IP/MAC list.									
<i>block</i>	Block packets from MAC addresses not in the IP/MAC list.									

## config firewall ipmacbinding table

Configure IP to MAC address pairs in the IP/MAC binding table.

```
config firewall ipmacbinding table
  Description: Configure IP to MAC address pairs in the IP/MAC binding table.
  edit <seq-num>
    set ip {ipv4-address}
    set mac {mac-address}
    set name {string}
    set status [enable|disable]
  next
end
```

## config firewall ipmacbinding table

Parameter	Description	Type	Size	Default
ip	IPv4 address portion of the pair (format: xxx.xxx.xxx.xxx).	ipv4-address	Not Specified	0.0.0.0
mac	MAC address portion of the pair (format = xx:xx:xx:xx:xx:xx in hexadecimal).	mac-address	Not Specified	00:00:00:00:00:00
name	Name of the pair.	string	Maximum length: 35	noname
seq-num	Entry number.	integer	Minimum value: 0 Maximum value: 4294967295	0
status	Enable/disable this IP-mac binding pair.	option	-	disable
		Option	Description	
		<i>enable</i>	Enable this IP-mac binding pair.	
		<i>disable</i>	Disable this IP-mac binding pair.	

## config firewall ippool

Configure IPv4 IP pools.

```
config firewall ippool
  Description: Configure IPv4 IP pools.
  edit <name>
    set add-nat64-route [disable|enable]
    set arp-intf {string}
    set arp-reply [disable|enable]
    set associated-interface {string}
    set block-size {integer}
    set cgn-block-size {integer}
    set cgn-client-endip {var-string}
    set cgn-client-ipv6shift {integer}
    set cgn-client-startip {var-string}
    set cgn-fixedalloc [disable|enable]
    set cgn-overload [disable|enable]
    set cgn-port-end {integer}
    set cgn-port-start {integer}
    set cgn-spa [disable|enable]
    set comments {var-string}
    set endip {ipv4-address-any}
    set endport {integer}
    set nat64 [disable|enable]
    set num-blocks-per-user {integer}
    set pba-timeout {integer}
```

```

set permit-any-host [disable|enable]
set port-per-user {integer}
set source-endip {ipv4-address-any}
set source-startip {ipv4-address-any}
set startip {ipv4-address-any}
set startport {integer}
set subnet-broadcast-in-ippool [disable|enable]
set type [overload|one-to-one|...]
set utilization-alarm-clear {integer}
set utilization-alarm-raise {integer}
next
end

```

## config firewall ippool

Parameter	Description	Type	Size	Default						
add-nat64-route	Enable/disable adding NAT64 route.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable adding NAT64 route.</td></tr><tr><td><i>enable</i></td><td>Enable adding NAT64 route.</td></tr></table>	Option	Description	<i>disable</i>	Disable adding NAT64 route.	<i>enable</i>	Enable adding NAT64 route.			
Option	Description									
<i>disable</i>	Disable adding NAT64 route.									
<i>enable</i>	Enable adding NAT64 route.									
arp-intf	Select an interface from available options that will reply to ARP requests. (If blank, any is selected).	string	Maximum length: 15							
arp-reply	Enable/disable replying to ARP requests when an IP Pool is added to a policy.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable ARP reply.</td></tr><tr><td><i>enable</i></td><td>Enable ARP reply.</td></tr></table>	Option	Description	<i>disable</i>	Disable ARP reply.	<i>enable</i>	Enable ARP reply.			
Option	Description									
<i>disable</i>	Disable ARP reply.									
<i>enable</i>	Enable ARP reply.									
associated-interface	Associated interface name.	string	Maximum length: 15							
block-size	Number of addresses in a block.	integer	Minimum value: 64 Maximum value: 4096	128						
cgn-block-size *	Number of ports in a block.	integer	Minimum value: 64 Maximum value: 4096	128						
cgn-client-endip *	Final client IPv4 address (inclusive) (format xxx.xxx.xxx.xxx, Default: 0.0.0.0).	var-string	Maximum length: 255							

Parameter	Description	Type	Size	Default						
cgn-client-ipv6shift *	IPv6 shift for fixed-allocation.	integer	Minimum value: 0 Maximum value: 127	0						
cgn-client-startip *	First client IPv4 address (inclusive) (format xxx.xxx.xxx.xxx, Default: 0.0.0.0).	var-string	Maximum length: 255							
cgn-fixedalloc *	Enable/disable fixed-allocation mode.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable fixed-allocation mode.</td></tr><tr><td>enable</td><td>Enable fixed-allocation mode.</td></tr></table>	Option	Description	disable	Disable fixed-allocation mode.	enable	Enable fixed-allocation mode.			
Option	Description									
disable	Disable fixed-allocation mode.									
enable	Enable fixed-allocation mode.									
cgn-overload *	Enable/disable overload mode.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable overload mode.</td></tr><tr><td>enable</td><td>Enable overload mode.</td></tr></table>	Option	Description	disable	Disable overload mode.	enable	Enable overload mode.			
Option	Description									
disable	Disable overload mode.									
enable	Enable overload mode.									
cgn-port-end *	Ending public port can be allocated.	integer	Minimum value: 1024 Maximum value: 65535	65530						
cgn-port-start *	Starting public port can be allocated.	integer	Minimum value: 1024 Maximum value: 65535	5117						
cgn-spa *	Enable/disable single port allocation mode.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable SPA mode.</td></tr><tr><td>enable</td><td>Enable SPA mode.</td></tr></table>	Option	Description	disable	Disable SPA mode.	enable	Enable SPA mode.			
Option	Description									
disable	Disable SPA mode.									
enable	Enable SPA mode.									
comments	Comment.	var-string	Maximum length: 255							
endip	Final IPv4 address (inclusive) in the range for the address pool (format xxx.xxx.xxx.xxx, Default: 0.0.0.0).	ipv4-address-any	Not Specified	0.0.0.0						

Parameter	Description	Type	Size	Default						
endport	Final port number (inclusive) in the range for the address pool (Default: 65533).	integer	Minimum value: 5117 Maximum value: 65533	65533						
name	IP pool name.	string	Maximum length: 79							
nat64	Enable/disable NAT64.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable DNAT64.</td></tr><tr><td><i>enable</i></td><td>Enable DNAT64.</td></tr></table>	Option	Description	<i>disable</i>	Disable DNAT64.	<i>enable</i>	Enable DNAT64.			
Option	Description									
<i>disable</i>	Disable DNAT64.									
<i>enable</i>	Enable DNAT64.									
num-blocks-per-user	Number of addresses blocks that can be used by a user.	integer	Minimum value: 1 Maximum value: 128	8						
pba-timeout	Port block allocation timeout (seconds).	integer	Minimum value: 3 Maximum value: 300	30						
permit-any-host	Enable/disable full cone NAT.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable full cone NAT.</td></tr><tr><td><i>enable</i></td><td>Enable full cone NAT.</td></tr></table>	Option	Description	<i>disable</i>	Disable full cone NAT.	<i>enable</i>	Enable full cone NAT.			
Option	Description									
<i>disable</i>	Disable full cone NAT.									
<i>enable</i>	Enable full cone NAT.									
port-per-user	Number of port for each user.	integer	Minimum value: 32 Maximum value: 60416	0						
source-endip	Final IPv4 address (inclusive) in the range of the source addresses to be translated (format xxx.xxx.xxx.xxx, Default: 0.0.0.0).	ipv4-address-any	Not Specified	0.0.0.0						
source-startip	First IPv4 address.	ipv4-address-any	Not Specified	0.0.0.0						

Parameter	Description	Type	Size	Default										
startip	First IPv4 address (inclusive) in the range for the address pool (format xxx.xxx.xxx.xxx, Default: 0.0.0.0).	ipv4-address-any	Not Specified	0.0.0.0										
startport	First port number (inclusive) in the range for the address pool (Default: 5117).	integer	Minimum value: 5117 Maximum value: 65533	5117										
subnet-broadcast-in-ippool	Enable/disable inclusion of the subnetwork address and broadcast IP address in the NAT64 IP pool.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Do not include the subnetwork address and broadcast IP address in the NAT64 IP pool.</td></tr><tr><td><i>enable</i></td><td>Include the subnetwork address and broadcast IP address in the NAT64 IP pool.</td></tr></table>				Option	Description	<i>disable</i>	Do not include the subnetwork address and broadcast IP address in the NAT64 IP pool.	<i>enable</i>	Include the subnetwork address and broadcast IP address in the NAT64 IP pool.				
Option	Description													
<i>disable</i>	Do not include the subnetwork address and broadcast IP address in the NAT64 IP pool.													
<i>enable</i>	Include the subnetwork address and broadcast IP address in the NAT64 IP pool.													
type	IP pool type (overload, one-to-one, fixed port range, or port block allocation).	option	-	overload										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>overload</i></td><td>IP addresses in the IP pool can be shared by clients.</td></tr><tr><td><i>one-to-one</i></td><td>One to one mapping.</td></tr><tr><td><i>fixed-port-range</i></td><td>Fixed port range.</td></tr><tr><td><i>port-block-allocation</i></td><td>Port block allocation.</td></tr></table>				Option	Description	<i>overload</i>	IP addresses in the IP pool can be shared by clients.	<i>one-to-one</i>	One to one mapping.	<i>fixed-port-range</i>	Fixed port range.	<i>port-block-allocation</i>	Port block allocation.
Option	Description													
<i>overload</i>	IP addresses in the IP pool can be shared by clients.													
<i>one-to-one</i>	One to one mapping.													
<i>fixed-port-range</i>	Fixed port range.													
<i>port-block-allocation</i>	Port block allocation.													
utilization-alarm-clear *	Pool utilization alarm clear threshold.	integer	Minimum value: 40 Maximum value: 100	80										
utilization-alarm-raise *	Pool utilization alarm raise threshold.	integer	Minimum value: 50 Maximum value: 100	100										

\* This parameter may not exist in some models.

## config firewall ippool6

Configure IPv6 IP pools.

```

config firewall ippool6
    Description: Configure IPv6 IP pools.
    edit <name>
        set add-nat46-route [disable|enable]
        set comments {var-string}
        set endip {ipv6-address}
        set nat46 [disable|enable]
        set startip {ipv6-address}
    next
end

```

## config firewall ippool6

Parameter	Description	Type	Size	Default
add-nat46-route	Enable/disable adding NAT46 route.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable adding NAT46 route.		
	<i>enable</i>	Enable adding NAT46 route.		
comments	Comment.	var-string	Maximum length: 255	
endip	Final IPv6 address.	ipv6-address	Not Specified	::
name	IPv6 IP pool name.	string	Maximum length: 79	
nat46	Enable/disable NAT46.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable NAT46.		
	<i>enable</i>	Enable NAT46.		
startip	First IPv6 address.	ipv6-address	Not Specified	::

## config firewall ippool\_grp



This command is available for model(s): FortiGate 2600F.

It is not available for: FortiGate 1000D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

Configure IPv4 pool groups.

```
config firewall ippool_grp
    Description: Configure IPv4 pool groups.
    edit <name>
        set uuid {uuid}
        set comments {var-string}
        set member <name1>, <name2>, ...
    next
end
```

## config firewall ippool\_grp

Parameter	Description	Type	Size	Default
name	.	string	Maximum length: 35	
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000
comments	Comment.	var-string	Maximum length: 255	



Parameter	Description	Type	Size	Default
member <name>	Member IP pool of the group (They must have same attributes except public/client ranges). IP pool name.	string	Maximum length: 79	

## config firewall ipv6-eh-filter

Configure IPv6 extension header filter.

```
config firewall ipv6-eh-filter
    Description: Configure IPv6 extension header filter.
    set auth [enable|disable]
    set dest-opt [enable|disable]
    set fragment [enable|disable]
    set hdopt-type {integer}
    set hop-opt [enable|disable]
    set no-next [enable|disable]
    set routing [enable|disable]
    set routing-type {integer}
end
```

## config firewall ipv6-eh-filter

Parameter	Description	Type	Size	Default						
auth	Enable/disable blocking packets with the Authentication header.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Block packets with the Authentication header.</td></tr><tr><td><i>disable</i></td><td>Allow packets with the Authentication header.</td></tr></table>	Option	Description	<i>enable</i>	Block packets with the Authentication header.	<i>disable</i>	Allow packets with the Authentication header.			
Option	Description									
<i>enable</i>	Block packets with the Authentication header.									
<i>disable</i>	Allow packets with the Authentication header.									
dest-opt	Enable/disable blocking packets with Destination Options headers.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable blocking packets with Destination Options headers.</td></tr><tr><td><i>disable</i></td><td>Disable blocking packets with Destination Options headers.</td></tr></table>	Option	Description	<i>enable</i>	Enable blocking packets with Destination Options headers.	<i>disable</i>	Disable blocking packets with Destination Options headers.			
Option	Description									
<i>enable</i>	Enable blocking packets with Destination Options headers.									
<i>disable</i>	Disable blocking packets with Destination Options headers.									
fragment	Enable/disable blocking packets with the Fragment header.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Block packets with the Fragment header.</td></tr><tr><td><i>disable</i></td><td>Allow packets with the Fragment header.</td></tr></table>	Option	Description	<i>enable</i>	Block packets with the Fragment header.	<i>disable</i>	Allow packets with the Fragment header.			
Option	Description									
<i>enable</i>	Block packets with the Fragment header.									
<i>disable</i>	Allow packets with the Fragment header.									

Parameter	Description	Type	Size	Default						
hdopt-type	Block specific Hop-by-Hop and/or Destination Option types (max. 7 types, each between 0 and 255).	integer	Minimum value: 0 Maximum value: 255							
hop-opt	Enable/disable blocking packets with the Hop-by-Hop Options header.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable blocking packets with the Hop-by-Hop Options header.</td></tr><tr><td><i>disable</i></td><td>Disable blocking packets with the Hop-by-Hop Options header.</td></tr></table>	Option	Description	<i>enable</i>	Enable blocking packets with the Hop-by-Hop Options header.	<i>disable</i>	Disable blocking packets with the Hop-by-Hop Options header.			
Option	Description									
<i>enable</i>	Enable blocking packets with the Hop-by-Hop Options header.									
<i>disable</i>	Disable blocking packets with the Hop-by-Hop Options header.									
no-next	Enable/disable blocking packets with the No Next header.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Block packets with the No Next header.</td></tr><tr><td><i>disable</i></td><td>Allow packets with the No Next header.</td></tr></table>	Option	Description	<i>enable</i>	Block packets with the No Next header.	<i>disable</i>	Allow packets with the No Next header.			
Option	Description									
<i>enable</i>	Block packets with the No Next header.									
<i>disable</i>	Allow packets with the No Next header.									
routing	Enable/disable blocking packets with Routing headers.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Block packets with Routing headers.</td></tr><tr><td><i>disable</i></td><td>Allow packets with Routing headers.</td></tr></table>	Option	Description	<i>enable</i>	Block packets with Routing headers.	<i>disable</i>	Allow packets with Routing headers.			
Option	Description									
<i>enable</i>	Block packets with Routing headers.									
<i>disable</i>	Allow packets with Routing headers.									
routing-type	Block specific Routing header types.	integer	Minimum value: 0 Maximum value: 255	0						

## config firewall ldb-monitor

Configure server load balancing health monitors.

```
config firewall ldb-monitor
  Description: Configure server load balancing health monitors.
  edit <name>
    set dns-match-ip {ipv4-address}
    set dns-protocol [udp|tcp]
    set dns-request-domain {string}
    set http-get {string}
    set http-match {string}
    set http-max-redirects {integer}
    set interval {integer}
    set port {integer}
    set retry {integer}
    set src-ip {ipv4-address}
```

```

        set timeout {integer}
        set type [ping|tcp|...]
    next
end

```

## config firewall ldb-monitor

Parameter	Description	Type	Size	Default						
dns-match-ip	Response IP expected from DNS server.	ipv4-address	Not Specified	0.0.0.0						
dns-protocol	Select the protocol used by the DNS health check monitor to check the health of the server (UDP   TCP).	option	-	udp						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>udp</td><td>UDP.</td></tr><tr><td>tcp</td><td>TCP.</td></tr></table>				Option	Description	udp	UDP.	tcp	TCP.
	Option	Description								
	udp	UDP.								
tcp	TCP.									
dns-request-domain	Fully qualified domain name to resolve for the DNS probe.	string	Maximum length: 255							
http-get	URL used to send a GET request to check the health of an HTTP server.	string	Maximum length: 255							
http-match	String to match the value expected in response to an HTTP-GET request.	string	Maximum length: 255							
http-max-redirects	The maximum number of HTTP redirects to be allowed.	integer	Minimum value: 0 Maximum value: 5	0						
interval	Time between health checks.	integer	Minimum value: 5 Maximum value: 65535	10						
name	Monitor name.	string	Maximum length: 35							
port	Service port used to perform the health check. If 0, health check monitor inherits port configured for the server.	integer	Minimum value: 0 Maximum value: 65535	0						
retry	Number health check attempts before the server is considered down.	integer	Minimum value: 1 Maximum value: 255	3						

Parameter	Description	Type	Size	Default												
src-ip	Source IP for Idb-monitor.	ipv4-address	Not Specified	0.0.0.0												
timeout	Time to wait to receive response to a health check from a server. Reaching the timeout means the health check failed.	integer	Minimum value: 1 Maximum value: 255	2												
type	Select the Monitor type used by the health check monitor to check the health of the server (PING   TCP   HTTP   HTTPS   DNS).	option	-													
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ping</td><td>PING health monitor.</td></tr><tr><td>tcp</td><td>TCP-connect health monitor.</td></tr><tr><td>http</td><td>HTTP-GET health monitor.</td></tr><tr><td>https</td><td>HTTP-GET health monitor with SSL.</td></tr><tr><td>dns</td><td>DNS health monitor.</td></tr></table>				Option	Description	ping	PING health monitor.	tcp	TCP-connect health monitor.	http	HTTP-GET health monitor.	https	HTTP-GET health monitor with SSL.	dns	DNS health monitor.
Option	Description															
ping	PING health monitor.															
tcp	TCP-connect health monitor.															
http	HTTP-GET health monitor.															
https	HTTP-GET health monitor with SSL.															
dns	DNS health monitor.															

## config firewall local-in-policy

Configure user defined IPv4 local-in policies.

```
config firewall local-in-policy
  Description: Configure user defined IPv4 local-in policies.
  edit <policyid>
    set action [accept|deny]
    set comments {var-string}
    set dstaddr <name1>, <name2>, ...
    set dstaddr-negate [enable|disable]
    set ha-mgmt-intf-only [enable|disable]
    set intf {string}
    set schedule {string}
    set service <name1>, <name2>, ...
    set service-negate [enable|disable]
    set srcaddr <name1>, <name2>, ...
    set srcaddr-negate [enable|disable]
    set status [enable|disable]
    set uuid {uuid}
  next
end
```

## config firewall local-in-policy

Parameter	Description	Type	Size	Default
action	Action performed on traffic matching the policy.	option	-	deny
	<b>Option</b>	<b>Description</b>		
	<i>accept</i>	Allow traffic matching this policy.		
	<i>deny</i>	Deny or block traffic matching this policy.		
comments	Comment.	var-string	Maximum length: 1023	
dstaddr <name>	Destination address object from available options. Address name.	string	Maximum length: 79	
dstaddr-negate	When enabled dstaddr specifies what the destination address must NOT be.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable destination address negate.		
	<i>disable</i>	Disable destination address negate.		
ha-mgmt-intf-only	Enable/disable dedicating the HA management interface only for local-in policy.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable dedicating HA management interface only for local-in policy.		
	<i>disable</i>	Disable dedicating HA management interface only for local-in policy.		
intf	Incoming interface name from available options.	string	Maximum length: 35	
policyid	User defined local in policy ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
schedule	Schedule object from available options.	string	Maximum length: 35	
service <name>	Service object from available options. Service name.	string	Maximum length: 79	
service-negate	When enabled service specifies what the service must NOT be.	option	-	disable

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable negated service match.		
	<i>disable</i>	Disable negated service match.		
srcaddr <name>	Source address object from available options. Address name.	string	Maximum length: 79	
srcaddr- negate	When enabled srcaddr specifies what the source address must NOT be.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable source address negate.		
	<i>disable</i>	Disable source address negate.		
status	Enable/disable this local-in policy.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable this local-in policy.		
	<i>disable</i>	Disable this local-in policy.		
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000- 0000-0000- 000000000000

## config firewall local-in-policy6

Configure user defined IPv6 local-in policies.

```
config firewall local-in-policy6
    Description: Configure user defined IPv6 local-in policies.
    edit <policyid>
        set action [accept|deny]
        set comments {var-string}
        set dstaddr <name1>, <name2>, ...
        set dstaddr-negate [enable|disable]
        set intf {string}
        set schedule {string}
        set service <name1>, <name2>, ...
        set service-negate [enable|disable]
        set srcaddr <name1>, <name2>, ...
        set srcaddr-negate [enable|disable]
        set status [enable|disable]
        set uuid {uuid}
    next
end
```

## config firewall local-in-policy6

Parameter	Description	Type	Size	Default
action	Action performed on traffic matching the policy.	option	-	deny
	<b>Option</b>	<b>Description</b>		
	<i>accept</i>	Allow local-in traffic matching this policy.		
	<i>deny</i>	Deny or block local-in traffic matching this policy.		
comments	Comment.	var-string	Maximum length: 1023	
dstaddr <name>	Destination address object from available options. Address name.	string	Maximum length: 79	
dstaddr-negate	When enabled dstaddr specifies what the destination address must NOT be.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable destination address negate.		
	<i>disable</i>	Disable destination address negate.		
intf	Incoming interface name from available options.	string	Maximum length: 35	
policyid	User defined local in policy ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
schedule	Schedule object from available options.	string	Maximum length: 35	
service <name>	Service object from available options. Separate names with a space. Service name.	string	Maximum length: 79	
service-negate	When enabled service specifies what the service must NOT be.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable negated service match.		
	<i>disable</i>	Disable negated service match.		
srcaddr <name>	Source address object from available options. Address name.	string	Maximum length: 79	

Parameter	Description	Type	Size	Default
srcaddr-negate	When enabled srcaddr specifies what the source address must NOT be.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable source address negate.		
	<i>disable</i>	Disable source address negate.		
status	Enable/disable this local-in policy.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable this local-in policy.		
	<i>disable</i>	Disable this local-in policy.		
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000

## config firewall multicast-address

Configure multicast addresses.

```
config firewall multicast-address
    Description: Configure multicast addresses.
    edit <name>
        set associated-interface {string}
        set color {integer}
        set comment {var-string}
        set end-ip {ipv4-address-any}
        set start-ip {ipv4-address-any}
        set subnet {ipv4-classnet-any}
        config tagging
            Description: Config object tagging.
            edit <name>
                set category {string}
                set tags <name1>, <name2>, ...
            next
        end
        set type [multicastrange|broadcastmask]
    next
end
```



## config firewall multicast-address

Parameter	Description	Type	Size	Default
associated-interface	Interface associated with the address object. When setting up a policy, only addresses associated with this interface are available.	string	Maximum length: 35	
color	Integer value to determine the color of the icon in the GUI.	integer	Minimum value: 0 Maximum value: 32	0
comment	Comment.	var-string	Maximum length: 255	
end-ip	Final IPv4 address (inclusive) in the range for the address.	ipv4-address-any	Not Specified	0.0.0.0
name	Multicast address name.	string	Maximum length: 79	
start-ip	First IPv4 address (inclusive) in the range for the address.	ipv4-address-any	Not Specified	0.0.0.0
subnet	Broadcast address and subnet.	ipv4-classnet-any	Not Specified	0.0.0.0 0.0.0.0
type	Type of address object: multicast IP address range or broadcast IP/mask to be treated as a multicast address.	option	-	multicastrange
		Option	Description	
		<i>multicastrange</i>	Multicast range.	
		<i>broadcastmask</i>	Broadcast IP/mask.	

## config tagging

Parameter	Description	Type	Size	Default
name	Tagging entry name.	string	Maximum length: 63	
category	Tag category.	string	Maximum length: 63	
tags <name>	Tags. Tag name.	string	Maximum length: 79	

## config firewall multicast-address6

Configure IPv6 multicast address.

```
config firewall multicast-address6
  Description: Configure IPv6 multicast address.
  edit <name>
    set color {integer}
    set comment {var-string}
    set ip6 {ipv6-network}
    config tagging
      Description: Config object tagging.
      edit <name>
        set category {string}
        set tags <name1>, <name2>, ...
      next
    end
  next
end
```

## config firewall multicast-address6

Parameter	Description	Type	Size	Default
color	Color of icon on the GUI.	integer	Minimum value: 0 Maximum value: 32	0
comment	Comment.	var-string	Maximum length: 255	
ip6	IPv6 address prefix (format: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/xxx).	ipv6-network	Not Specified	::/0
name	IPv6 multicast address name.	string	Maximum length: 79	

## config tagging

Parameter	Description	Type	Size	Default
name	Tagging entry name.	string	Maximum length: 63	
category	Tag category.	string	Maximum length: 63	
tags <name>	Tags. Tag name.	string	Maximum length: 79	

## config firewall multicast-policy

Configure multicast NAT policies.

```
config firewall multicast-policy
  Description: Configure multicast NAT policies.
  edit <id>
    set action [accept|deny]
    set auto-asic-offload [enable|disable]
    set comments {var-string}
    set dnat {ipv4-address-any}
    set dstaddr <name1>, <name2>, ...
    set dstintf {string}
    set end-port {integer}
    set logtraffic [enable|disable]
    set name {string}
    set protocol {integer}
    set snat [enable|disable]
    set snat-ip {ipv4-address}
    set srcaddr <name1>, <name2>, ...
    set srcintf {string}
    set start-port {integer}
    set status [enable|disable]
    set uuid {uuid}
  next
end
```

## config firewall multicast-policy

Parameter	Description	Type	Size	Default
action	Accept or deny traffic matching the policy.	option	-	accept
	<div><div>Option</div><div>Description</div></div>			
	<i>accept</i>	Accept traffic matching the policy.		
	<i>deny</i>	Deny or block traffic matching the policy.		
auto-asic-offload *	Enable/disable offloading policy traffic for hardware acceleration.	option	-	enable
	<div><div>Option</div><div>Description</div></div>			
	<i>enable</i>	Enable hardware acceleration offloading.		
	<i>disable</i>	Disable offloading for hardware acceleration.		
comments	Comment.	var-string	Maximum length: 1023	
dnat	IPv4 DNAT address used for multicast destination addresses.	ipv4-address-any	Not Specified	0.0.0.0

Parameter	Description	Type	Size	Default						
dstaddr <name>	Destination address objects. Destination address objects.	string	Maximum length: 79							
dstintf	Destination interface name.	string	Maximum length: 35							
end-port	Integer value for ending TCP/UDP/SCTP destination port in range.	integer	Minimum value: 0 Maximum value: 65535	65535						
id	Policy ID.	integer	Minimum value: 0 Maximum value: 4294967294	0						
logtraffic	Enable/disable logging traffic accepted by this policy.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable logging traffic accepted by this policy.</td></tr><tr><td><i>disable</i></td><td>Disable logging traffic accepted by this policy.</td></tr></table>				Option	Description	<i>enable</i>	Enable logging traffic accepted by this policy.	<i>disable</i>	Disable logging traffic accepted by this policy.
Option	Description									
<i>enable</i>	Enable logging traffic accepted by this policy.									
<i>disable</i>	Disable logging traffic accepted by this policy.									
name	Policy name.	string	Maximum length: 35							
protocol	Integer value for the protocol type as defined by IANA.	integer	Minimum value: 0 Maximum value: 255	0						
snat	Enable/disable substitution of the outgoing interface IP address for the original source IP address (called source NAT or SNAT).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable source NAT.</td></tr><tr><td><i>disable</i></td><td>Disable source NAT.</td></tr></table>				Option	Description	<i>enable</i>	Enable source NAT.	<i>disable</i>	Disable source NAT.
Option	Description									
<i>enable</i>	Enable source NAT.									
<i>disable</i>	Disable source NAT.									
snat-ip	IPv4 address to be used as the source address for NATed traffic.	ipv4- address	Not Specified	0.0.0.0						
srcaddr <name>	Source address objects. Source address objects.	string	Maximum length: 79							
srcintf	Source interface name.	string	Maximum length: 35							

Parameter	Description	Type	Size	Default						
start-port	Integer value for starting TCP/UDP/SCTP destination port in range.	integer	Minimum value: 0 Maximum value: 65535	1						
status	Enable/disable this policy.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable this policy.</td></tr><tr><td><i>disable</i></td><td>Disable this policy.</td></tr></table>				Option	Description	<i>enable</i>	Enable this policy.	<i>disable</i>	Disable this policy.
	Option	Description								
	<i>enable</i>	Enable this policy.								
<i>disable</i>	Disable this policy.									
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000						

\* This parameter may not exist in some models.

## config firewall multicast-policy6

Configure IPv6 multicast NAT policies.

```
config firewall multicast-policy6
    Description: Configure IPv6 multicast NAT policies.
    edit <id>
        set action [accept|deny]
        set auto-asic-offload [enable|disable]
        set comments {var-string}
        set dstaddr <name1>, <name2>, ...
        set dstintf {string}
        set end-port {integer}
        set logtraffic [enable|disable]
        set name {string}
        set protocol {integer}
        set srcaddr <name1>, <name2>, ...
        set srcintf {string}
        set start-port {integer}
        set status [enable|disable]
        set uuid {uuid}
    next
end
```

## config firewall multicast-policy6

Parameter	Description	Type	Size	Default
action	Accept or deny traffic matching the policy.	option	-	accept

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>accept</i></td><td>Accept.</td></tr><tr><td><i>deny</i></td><td>Deny.</td></tr></table>	Option	Description	<i>accept</i>	Accept.	<i>deny</i>	Deny.			
	Option	Description								
	<i>accept</i>	Accept.								
<i>deny</i>	Deny.									
auto-asic-offload *	Enable/disable offloading policy traffic for hardware acceleration.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable offloading policy traffic for hardware acceleration.</td></tr><tr><td><i>disable</i></td><td>Disable offloading policy traffic for hardware acceleration.</td></tr></table>	Option	Description	<i>enable</i>	Enable offloading policy traffic for hardware acceleration.	<i>disable</i>	Disable offloading policy traffic for hardware acceleration.			
	Option	Description								
	<i>enable</i>	Enable offloading policy traffic for hardware acceleration.								
<i>disable</i>	Disable offloading policy traffic for hardware acceleration.									
comments	Comment.	var-string	Maximum length: 1023							
dstaddr <name>	IPv6 destination address name. Address name.	string	Maximum length: 79							
dstintf	IPv6 destination interface name.	string	Maximum length: 35							
end-port	Integer value for ending TCP/UDP/SCTP destination port in range.	integer	Minimum value: 0 Maximum value: 65535	65535						
id	Policy ID.	integer	Minimum value: 0 Maximum value: 4294967294	0						
logtraffic	Enable/disable logging traffic accepted by this policy.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable logging traffic accepted by this policy.</td></tr><tr><td><i>disable</i></td><td>Disable logging traffic accepted by this policy.</td></tr></table>	Option	Description	<i>enable</i>	Enable logging traffic accepted by this policy.	<i>disable</i>	Disable logging traffic accepted by this policy.			
	Option	Description								
	<i>enable</i>	Enable logging traffic accepted by this policy.								
<i>disable</i>	Disable logging traffic accepted by this policy.									
name	Policy name.	string	Maximum length: 35							
protocol	Integer value for the protocol type as defined by IANA.	integer	Minimum value: 0 Maximum value: 255	0						

Parameter	Description	Type	Size	Default						
srcaddr <name>	IPv6 source address name. Address name.	string	Maximum length: 79							
srcintf	IPv6 source interface name.	string	Maximum length: 35							
start-port	Integer value for starting TCP/UDP/SCTP destination port in range.	integer	Minimum value: 0 Maximum value: 65535	1						
status	Enable/disable this policy.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable this policy.</td></tr><tr><td><i>disable</i></td><td>Disable this policy.</td></tr></table>				Option	Description	<i>enable</i>	Enable this policy.	<i>disable</i>	Disable this policy.
Option	Description									
<i>enable</i>	Enable this policy.									
<i>disable</i>	Disable this policy.									
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000- 0000-0000- 000000000000						

\* This parameter may not exist in some models.

## config firewall pfcp



This command is available for model(s): FortiGate 2600F, FortiGate 3000F, FortiGate 3001F, FortiGate 3400E.

It is not available for: FortiGate 1000D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2601F, FortiGate 3000D, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3900E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

## Configure PFCP.

```
config firewall pfc
  Description: Configure PFCP.
  edit <name>
    set denied-log [enable|disable]
    set forwarded-log [enable|disable]
    set invalid-reserved-field [allow|deny]
    set log-freq {integer}
    set max-message-length {integer}
    set message-filter {string}
    set min-message-length {integer}
    set monitor-mode [enable|disable|...]
    set pfc-timeout {integer}
    set traffic-count-log [enable|disable]
    set unknown-version [allow|deny]
  next
end
```

## config firewall pfc

Parameter	Description	Type	Size	Default						
denied-log	Enable/disable logging denied PFCP packets.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
	Option	Description								
	<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.									
forwarded-log	Enable/disable logging forwarded PFCP packets.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
	Option	Description								
	<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.									
invalid-reserved-field	Allow or deny invalid reserved field in PFCP header packets.	option	-	deny						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow setting.</td></tr><tr><td><i>deny</i></td><td>Deny setting.</td></tr></table>	Option	Description	<i>allow</i>	Allow setting.	<i>deny</i>	Deny setting.			
	Option	Description								
	<i>allow</i>	Allow setting.								
<i>deny</i>	Deny setting.									
log-freq	Logging frequency of PFCP packets.	integer	Minimum value: 0 Maximum value: 4294967295	0						



Parameter	Description	Type	Size	Default								
max-message-length	Maximum message length.	integer	Minimum value: 0 Maximum value: 4294967295	1452								
message-filter	PFCP message filter.	string	Maximum length: 63									
min-message-length	Minimum message length.	integer	Minimum value: 0 Maximum value: 4294967295	0								
monitor-mode	PFCP monitor mode.	option	-	vdom								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable PFCP monitor mode.</td></tr><tr><td><i>disable</i></td><td>Disable PFCP monitor mode.</td></tr><tr><td><i>vdom</i></td><td>Enable/disable PFCP monitor mode based on VDOM setting.</td></tr></table>				Option	Description	<i>enable</i>	Enable PFCP monitor mode.	<i>disable</i>	Disable PFCP monitor mode.	<i>vdom</i>	Enable/disable PFCP monitor mode based on VDOM setting.
Option	Description											
<i>enable</i>	Enable PFCP monitor mode.											
<i>disable</i>	Disable PFCP monitor mode.											
<i>vdom</i>	Enable/disable PFCP monitor mode based on VDOM setting.											
name	PFCP profile name.	string	Maximum length: 63									
pfcp-timeout	Set PFCP timeout (in seconds).	integer	Minimum value: 0 Maximum value: 4294967295	86400								
traffic-count-log	Enable/disable logging session traffic counter.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>				Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
unknown-version	Allow or deny unknown version packets.	option	-	allow								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow setting.</td></tr><tr><td><i>deny</i></td><td>Deny setting.</td></tr></table>				Option	Description	<i>allow</i>	Allow setting.	<i>deny</i>	Deny setting.		
Option	Description											
<i>allow</i>	Allow setting.											
<i>deny</i>	Deny setting.											

---

## config firewall policy

Configure IPv4/IPv6 policies.

```
config firewall policy
  Description: Configure IPv4/IPv6 policies.
  edit <policyid>
    set action [accept|deny|...]
    set anti-replay [enable|disable]
    set application-list {string}
    set auth-cert {string}
    set auth-path [enable|disable]
    set auth-redirect-addr {string}
    set auto-asic-offload [enable|disable]
    set av-profile {string}
    set block-notification [enable|disable]
    set captive-portal-exempt [enable|disable]
    set capture-packet [enable|disable]
    set cgn-eif [enable|disable]
    set cgn-eim [enable|disable]
    set cgn-log-server-grp {string}
    set cgn-resource-quota {integer}
    set cgn-session-quota {integer}
    set cifs-profile {string}
    set comments {var-string}
    set custom-log-fields <field-id1>, <field-id2>, ...
    set decrypted-traffic-mirror {string}
    set delay-tcp-npu-session [enable|disable]
    set diffserv-forward [enable|disable]
    set diffserv-reverse [enable|disable]
    set diffservcode-forward {user}
    set diffservcode-rev {user}
    set disclaimer [enable|disable]
    set dlp-sensor {string}
    set dnsfilter-profile {string}
    set dsri [enable|disable]
    set dstaddr <name1>, <name2>, ...
    set dstaddr-negate [enable|disable]
    set dstaddr6 <name1>, <name2>, ...
    set dstintf <name1>, <name2>, ...
    set dynamic-shaping [enable|disable]
    set email-collect [enable|disable]
    set emailfilter-profile {string}
    set fec [enable|disable]
    set file-filter-profile {string}
    set firewall-session-dirty [check-all|check-new]
    set fixedport [enable|disable]
    set fsso-agent-for-ntlm {string}
    set fsso-groups <name1>, <name2>, ...
    set geoip-anycast [enable|disable]
    set geoip-match [physical-location|registered-location]
    set groups <name1>, <name2>, ...
    set gtp-profile {string}
    set http-policy-redirect [enable|disable]
    set icap-profile {string}
    set identity-based-route {string}
```

---

```
set inbound [enable|disable]
set inspection-mode [proxy|flow]
set internet-service [enable|disable]
set internet-service-custom <name1>, <name2>, ...
set internet-service-custom-group <name1>, <name2>, ...
set internet-service-group <name1>, <name2>, ...
set internet-service-name <name1>, <name2>, ...
set internet-service-negate [enable|disable]
set internet-service-src [enable|disable]
set internet-service-src-custom <name1>, <name2>, ...
set internet-service-src-custom-group <name1>, <name2>, ...
set internet-service-src-group <name1>, <name2>, ...
set internet-service-src-name <name1>, <name2>, ...
set internet-service-src-negate [enable|disable]
set ippool [enable|disable]
set ips-sensor {string}
set logtraffic [all|utm|...]
set logtraffic-start [enable|disable]
set match-vip [enable|disable]
set match-vip-only [enable|disable]
set name {string}
set nat [enable|disable]
set nat46 [enable|disable]
set nat64 [enable|disable]
set natinbound [enable|disable]
set natip {ipv4-classnet}
set natoutbound [enable|disable]
set np-acceleration [enable|disable]
set ntlm [enable|disable]
set ntlm-enabled-browsers <user-agent-string1>, <user-agent-string2>, ...
set ntlm-guest [enable|disable]
set outbound [enable|disable]
set passive-wan-health-measurement [enable|disable]
set per-ip-shaper {string}
set permit-any-host [enable|disable]
set permit-stun-host [enable|disable]
set pfc-p-profile {string}
set policy-offload [enable|disable]
set poolname <name1>, <name2>, ...
set poolname6 <name1>, <name2>, ...
set profile-group {string}
set profile-protocol-options {string}
set profile-type [single|group]
set radius-mac-auth-bypass [enable|disable]
set redirect-url {var-string}
set replacemsg-override-group {string}
set reputation-direction [source|destination]
set reputation-minimum {integer}
set rtp-addr <name1>, <name2>, ...
set rtp-nat [disable|enable]
set schedule {string}
set schedule-timeout [enable|disable]
set sctp-filter-profile {string}
set send-deny-packet [disable|enable]
set service <name1>, <name2>, ...
set service-negate [enable|disable]
```

```

set session-ttl {user}
set sgt <id1>, <id2>, ...
set sgt-check [enable|disable]
set src-vendor-mac <id1>, <id2>, ...
set srcaddr <name1>, <name2>, ...
set srcaddr-negate [enable|disable]
set srcaddr6 <name1>, <name2>, ...
set srcintf <name1>, <name2>, ...
set ssh-filter-profile {string}
set ssh-policy-redirect [enable|disable]
set ssl-ssh-profile {string}
set status [enable|disable]
set tcp-mss-receiver {integer}
set tcp-mss-sender {integer}
set tcp-session-without-syn [all|data-only|...]
set tcp-timeout-pid {integer}
set timeout-send-rst [enable|disable]
set tos {user}
set tos-mask {user}
set tos-negate [enable|disable]
set traffic-shaper {string}
set traffic-shaper-reverse {string}
set udp-timeout-pid {integer}
set users <name1>, <name2>, ...
set utm-status [enable|disable]
set uuid {uuid}
set videofilter-profile {string}
set vlan-cos-fwd {integer}
set vlan-cos-rev {integer}
set vlan-filter {user}
set voip-profile {string}
set vpntunnel {string}
set waf-profile {string}
set wanopt [enable|disable]
set wanopt-detection [active|passive|...]
set wanopt-passive-opt [default|transparent|...]
set wanopt-peer {string}
set wanopt-profile {string}
set wccp [enable|disable]
set webcache [enable|disable]
set webcache-https [disable|enable]
set webfilter-profile {string}
set webproxy-forward-server {string}
set webproxy-profile {string}
set ztna-ems-tag <name1>, <name2>, ...
set ztna-geo-tag <name1>, <name2>, ...
set ztna-status [enable|disable]

```

next

end

## config firewall policy

Parameter	Description	Type	Size	Default
action	Policy action (accept/deny/ipsec).	option	-	deny

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>accept</i></td><td>Allows session that match the firewall policy.</td></tr><tr><td><i>deny</i></td><td>Blocks sessions that match the firewall policy.</td></tr><tr><td><i>ipsec</i></td><td>Firewall policy becomes a policy-based IPsec VPN policy.</td></tr></table>	Option	Description	<i>accept</i>	Allows session that match the firewall policy.	<i>deny</i>	Blocks sessions that match the firewall policy.	<i>ipsec</i>	Firewall policy becomes a policy-based IPsec VPN policy.			
	Option	Description										
	<i>accept</i>	Allows session that match the firewall policy.										
	<i>deny</i>	Blocks sessions that match the firewall policy.										
<i>ipsec</i>	Firewall policy becomes a policy-based IPsec VPN policy.											
anti-replay	Enable/disable anti-replay check.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable anti-replay check.</td></tr><tr><td><i>disable</i></td><td>Disable anti-replay check.</td></tr></table>	Option	Description	<i>enable</i>	Enable anti-replay check.	<i>disable</i>	Disable anti-replay check.					
	Option	Description										
	<i>enable</i>	Enable anti-replay check.										
<i>disable</i>	Disable anti-replay check.											
application-list	Name of an existing Application list.	string	Maximum length: 35									
auth-cert	HTTPS server certificate for policy authentication.	string	Maximum length: 35									
auth-path	Enable/disable authentication-based routing.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable authentication-based routing.</td></tr><tr><td><i>disable</i></td><td>Disable authentication-based routing.</td></tr></table>	Option	Description	<i>enable</i>	Enable authentication-based routing.	<i>disable</i>	Disable authentication-based routing.					
	Option	Description										
	<i>enable</i>	Enable authentication-based routing.										
<i>disable</i>	Disable authentication-based routing.											
auth-redirect-addr	HTTP-to-HTTPS redirect address for firewall authentication.	string	Maximum length: 63									
auto-asic-offload *	Enable/disable policy traffic ASIC offloading.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable auto ASIC offloading.</td></tr><tr><td><i>disable</i></td><td>Disable ASIC offloading.</td></tr></table>	Option	Description	<i>enable</i>	Enable auto ASIC offloading.	<i>disable</i>	Disable ASIC offloading.					
	Option	Description										
	<i>enable</i>	Enable auto ASIC offloading.										
<i>disable</i>	Disable ASIC offloading.											
av-profile	Name of an existing Antivirus profile.	string	Maximum length: 35									
block-notification	Enable/disable block notification.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
	Option	Description										
	<i>enable</i>	Enable setting.										
<i>disable</i>	Disable setting.											

Parameter	Description	Type	Size	Default						
captive-portal-exempt	Enable to exempt some users from the captive portal.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable exemption of captive portal.</td></tr><tr><td><i>disable</i></td><td>Disable exemption of captive portal.</td></tr></table>	Option	Description	<i>enable</i>	Enable exemption of captive portal.	<i>disable</i>	Disable exemption of captive portal.			
Option	Description									
<i>enable</i>	Enable exemption of captive portal.									
<i>disable</i>	Disable exemption of captive portal.									
capture-packet *	Enable/disable capture packets.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable capture packets.</td></tr><tr><td><i>disable</i></td><td>Disable capture packets.</td></tr></table>	Option	Description	<i>enable</i>	Enable capture packets.	<i>disable</i>	Disable capture packets.			
Option	Description									
<i>enable</i>	Enable capture packets.									
<i>disable</i>	Disable capture packets.									
cg-nat-eif *	Enable/Disable CGN endpoint independent filtering.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable nat EIF.</td></tr><tr><td><i>disable</i></td><td>Disable nat EIF.</td></tr></table>	Option	Description	<i>enable</i>	Enable nat EIF.	<i>disable</i>	Disable nat EIF.			
Option	Description									
<i>enable</i>	Enable nat EIF.									
<i>disable</i>	Disable nat EIF.									
cg-nat-eim *	Enable/Disable CGN endpoint independent mapping	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable nat EIM.</td></tr><tr><td><i>disable</i></td><td>Disable nat EIM.</td></tr></table>	Option	Description	<i>enable</i>	Enable nat EIM.	<i>disable</i>	Disable nat EIM.			
Option	Description									
<i>enable</i>	Enable nat EIM.									
<i>disable</i>	Disable nat EIM.									
cg-nat-log-server-grp *	NP log server group name	string	Maximum length: 35							
cg-nat-resource-quota *	resource quota	integer	Minimum value: 1 Maximum value: 16	16						
cg-nat-session-quota *	session quota	integer	Minimum value: 0 Maximum value: 16777215	16777215						
cifs-profile	Name of an existing CIFS profile.	string	Maximum length: 35							

Parameter	Description	Type	Size	Default						
comments	Comment.	var-string	Maximum length: 1023							
custom-log-fields <field-id>	Custom fields to append to log messages for this policy. Custom log field.	string	Maximum length: 35							
decrypted-traffic-mirror	Decrypted traffic mirror.	string	Maximum length: 35							
delay-tcp-npu-session	Enable TCP NPU session delay to guarantee packet order of 3-way handshake.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable TCP NPU session delay in order to guarantee packet order of 3-way handshake.</td></tr><tr><td><i>disable</i></td><td>Disable TCP NPU session delay in order to guarantee packet order of 3-way handshake.</td></tr></table>	Option	Description	<i>enable</i>	Enable TCP NPU session delay in order to guarantee packet order of 3-way handshake.	<i>disable</i>	Disable TCP NPU session delay in order to guarantee packet order of 3-way handshake.			
Option	Description									
<i>enable</i>	Enable TCP NPU session delay in order to guarantee packet order of 3-way handshake.									
<i>disable</i>	Disable TCP NPU session delay in order to guarantee packet order of 3-way handshake.									
diffserv-forward	Enable to change packet's DiffServ values to the specified diffservcode-forward value.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting forward (original) traffic Diffserv.</td></tr><tr><td><i>disable</i></td><td>Disable setting forward (original) traffic Diffserv.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting forward (original) traffic Diffserv.	<i>disable</i>	Disable setting forward (original) traffic Diffserv.			
Option	Description									
<i>enable</i>	Enable setting forward (original) traffic Diffserv.									
<i>disable</i>	Disable setting forward (original) traffic Diffserv.									
diffserv-reverse	Enable to change packet's reverse (reply) DiffServ values to the specified diffservcode-rev value.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting reverse (reply) traffic DiffServ.</td></tr><tr><td><i>disable</i></td><td>Disable setting reverse (reply) traffic DiffServ.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting reverse (reply) traffic DiffServ.	<i>disable</i>	Disable setting reverse (reply) traffic DiffServ.			
Option	Description									
<i>enable</i>	Enable setting reverse (reply) traffic DiffServ.									
<i>disable</i>	Disable setting reverse (reply) traffic DiffServ.									
diffservcode-forward	Change packet's DiffServ to this value.	user	Not Specified							
diffservcode-rev	Change packet's reverse (reply) DiffServ to this value.	user	Not Specified							
disclaimer	Enable/disable user authentication disclaimer.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable user authentication disclaimer.</td></tr><tr><td><i>disable</i></td><td>Disable user authentication disclaimer.</td></tr></table>	Option	Description	<i>enable</i>	Enable user authentication disclaimer.	<i>disable</i>	Disable user authentication disclaimer.			
Option	Description									
<i>enable</i>	Enable user authentication disclaimer.									
<i>disable</i>	Disable user authentication disclaimer.									

Parameter	Description	Type	Size	Default						
dlp-sensor	Name of an existing DLP sensor.	string	Maximum length: 35							
dnsfilter-profile	Name of an existing DNS filter profile.	string	Maximum length: 35							
dsri	Enable DSRI to ignore HTTP server responses.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable DSRI.</td></tr><tr><td><i>disable</i></td><td>Disable DSRI.</td></tr></table>	Option	Description	<i>enable</i>	Enable DSRI.	<i>disable</i>	Disable DSRI.			
Option	Description									
<i>enable</i>	Enable DSRI.									
<i>disable</i>	Disable DSRI.									
dstaddr <name>	Destination IPv4 address and address group names. Address name.	string	Maximum length: 79							
dstaddr-negate	When enabled dstaddr/dstaddr6 specifies what the destination address must NOT be.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable destination address negate.</td></tr><tr><td><i>disable</i></td><td>Disable destination address negate.</td></tr></table>	Option	Description	<i>enable</i>	Enable destination address negate.	<i>disable</i>	Disable destination address negate.			
Option	Description									
<i>enable</i>	Enable destination address negate.									
<i>disable</i>	Disable destination address negate.									
dstaddr6 <name>	Destination IPv6 address name and address group names. Address name.	string	Maximum length: 79							
dstintf <name>	Outgoing (egress) interface. Interface name.	string	Maximum length: 79							
dynamic-shaping	Enable/disable dynamic RADIUS defined traffic shaping.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable dynamic RADIUS defined traffic shaping.</td></tr><tr><td><i>disable</i></td><td>Disable dynamic RADIUS defined traffic shaping.</td></tr></table>	Option	Description	<i>enable</i>	Enable dynamic RADIUS defined traffic shaping.	<i>disable</i>	Disable dynamic RADIUS defined traffic shaping.			
Option	Description									
<i>enable</i>	Enable dynamic RADIUS defined traffic shaping.									
<i>disable</i>	Disable dynamic RADIUS defined traffic shaping.									
email-collect	Enable/disable email collection.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable email collection.</td></tr><tr><td><i>disable</i></td><td>Disable email collection.</td></tr></table>	Option	Description	<i>enable</i>	Enable email collection.	<i>disable</i>	Disable email collection.			
Option	Description									
<i>enable</i>	Enable email collection.									
<i>disable</i>	Disable email collection.									



Parameter	Description	Type	Size	Default						
emailfilter-profile	Name of an existing email filter profile.	string	Maximum length: 35							
fec	Enable/disable Forward Error Correction on traffic matching this policy on a FEC device.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Forward Error Correction.</td></tr><tr><td><i>disable</i></td><td>Disable Forward Error Correction.</td></tr></table>	Option	Description	<i>enable</i>	Enable Forward Error Correction.	<i>disable</i>	Disable Forward Error Correction.			
Option	Description									
<i>enable</i>	Enable Forward Error Correction.									
<i>disable</i>	Disable Forward Error Correction.									
file-filter-profile	Name of an existing file-filter profile.	string	Maximum length: 35							
firewall-session-dirty	How to handle sessions if the configuration of this firewall policy changes.	option	-	check-all						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>check-all</i></td><td>Flush all current sessions accepted by this policy. These sessions must be started and re-matched with policies.</td></tr><tr><td><i>check-new</i></td><td>Continue to allow sessions already accepted by this policy.</td></tr></table>	Option	Description	<i>check-all</i>	Flush all current sessions accepted by this policy. These sessions must be started and re-matched with policies.	<i>check-new</i>	Continue to allow sessions already accepted by this policy.			
Option	Description									
<i>check-all</i>	Flush all current sessions accepted by this policy. These sessions must be started and re-matched with policies.									
<i>check-new</i>	Continue to allow sessions already accepted by this policy.									
fixedport	Enable to prevent source NAT from changing a session's source port.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
fsso-agent-for-ntlm	FSSO agent to use for NTLM authentication.	string	Maximum length: 35							
fsso-groups <name>	Names of FSSO groups. Names of FSSO groups.	string	Maximum length: 511							
geoip-anycast	Enable/disable recognition of anycast IP addresses using the geography IP database.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable recognition of anycast IP addresses using the geography IP database.</td></tr><tr><td><i>disable</i></td><td>Disable recognition of anycast IP addresses using the geography IP database.</td></tr></table>	Option	Description	<i>enable</i>	Enable recognition of anycast IP addresses using the geography IP database.	<i>disable</i>	Disable recognition of anycast IP addresses using the geography IP database.			
Option	Description									
<i>enable</i>	Enable recognition of anycast IP addresses using the geography IP database.									
<i>disable</i>	Disable recognition of anycast IP addresses using the geography IP database.									
geoip-match	Match geography address based either on its physical location or registered location.	option	-	physical-location						

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>physical-location</i>	Match geography address to its physical location using the geography IP database.		
	<i>registered-location</i>	Match geography address to its registered location using the geography IP database.		
groups <name>	Names of user groups that can authenticate with this policy. Group name.	string	Maximum length: 79	
gtp-profile *	GTP profile.	string	Maximum length: 63	
http-policy-redirect	Redirect HTTP(S) traffic to matching transparent web proxy policy.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable HTTP(S) policy redirect.		
	<i>disable</i>	Disable HTTP(S) policy redirect.		
icap-profile	Name of an existing ICAP profile.	string	Maximum length: 35	
identity-based-route	Name of identity-based routing rule.	string	Maximum length: 35	
inbound	Policy-based IPsec VPN: only traffic from the remote network can initiate a VPN.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
inspection-mode	Policy inspection mode (Flow/proxy). Default is Flow mode.	option	-	flow
	<b>Option</b>	<b>Description</b>		
	<i>proxy</i>	Proxy based inspection.		
	<i>flow</i>	Flow based inspection.		
internet-service	Enable/disable use of Internet Services for this policy. If enabled, destination address and service are not used.	option	-	disable

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable use of Internet Services in policy.</td></tr><tr><td><i>disable</i></td><td>Disable use of Internet Services in policy.</td></tr></table>	Option	Description	<i>enable</i>	Enable use of Internet Services in policy.	<i>disable</i>	Disable use of Internet Services in policy.			
	Option	Description								
	<i>enable</i>	Enable use of Internet Services in policy.								
<i>disable</i>	Disable use of Internet Services in policy.									
internet-service-custom <name>	Custom Internet Service name. Custom Internet Service name.	string	Maximum length: 79							
internet-service-custom-group <name>	Custom Internet Service group name. Custom Internet Service group name.	string	Maximum length: 79							
internet-service-group <name>	Internet Service group name. Internet Service group name.	string	Maximum length: 79							
internet-service-name <name>	Internet Service name. Internet Service name.	string	Maximum length: 79							
internet-service-negate	When enabled internet-service specifies what the service must NOT be.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable negated Internet Service match.</td></tr><tr><td><i>disable</i></td><td>Disable negated Internet Service match.</td></tr></table>	Option	Description	<i>enable</i>	Enable negated Internet Service match.	<i>disable</i>	Disable negated Internet Service match.			
	Option	Description								
	<i>enable</i>	Enable negated Internet Service match.								
<i>disable</i>	Disable negated Internet Service match.									
internet-service-src	Enable/disable use of Internet Services in source for this policy. If enabled, source address is not used.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable use of Internet Services source in policy.</td></tr><tr><td><i>disable</i></td><td>Disable use of Internet Services source in policy.</td></tr></table>	Option	Description	<i>enable</i>	Enable use of Internet Services source in policy.	<i>disable</i>	Disable use of Internet Services source in policy.			
	Option	Description								
	<i>enable</i>	Enable use of Internet Services source in policy.								
<i>disable</i>	Disable use of Internet Services source in policy.									
internet-service-src-custom <name>	Custom Internet Service source name. Custom Internet Service name.	string	Maximum length: 79							
internet-service-src-custom-group <name>	Custom Internet Service source group name. Custom Internet Service group name.	string	Maximum length: 79							
internet-service-src-group <name>	Internet Service source group name. Internet Service group name.	string	Maximum length: 79							
internet-service-src-name <name>	Internet Service source name. Internet Service name.	string	Maximum length: 79							

Parameter	Description	Type	Size	Default								
internet-service-src-negate	When enabled internet-service-src specifies what the service must NOT be.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable negated Internet Service source match.</td></tr><tr><td><i>disable</i></td><td>Disable negated Internet Service source match.</td></tr></table>	Option	Description	<i>enable</i>	Enable negated Internet Service source match.	<i>disable</i>	Disable negated Internet Service source match.					
Option	Description											
<i>enable</i>	Enable negated Internet Service source match.											
<i>disable</i>	Disable negated Internet Service source match.											
ippool	Enable to use IP Pools for source NAT.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
ips-sensor	Name of an existing IPS sensor.	string	Maximum length: 35									
logtraffic	Enable or disable logging. Log all sessions or security profile sessions.	option	-	utm								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>all</i></td><td>Log all sessions accepted or denied by this policy.</td></tr><tr><td><i>utm</i></td><td>Log traffic that has a security profile applied to it.</td></tr><tr><td><i>disable</i></td><td>Disable all logging for this policy.</td></tr></table>	Option	Description	<i>all</i>	Log all sessions accepted or denied by this policy.	<i>utm</i>	Log traffic that has a security profile applied to it.	<i>disable</i>	Disable all logging for this policy.			
Option	Description											
<i>all</i>	Log all sessions accepted or denied by this policy.											
<i>utm</i>	Log traffic that has a security profile applied to it.											
<i>disable</i>	Disable all logging for this policy.											
logtraffic-start	Record logs when a session starts.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
match-vip	Enable to match packets that have had their destination addresses changed by a VIP.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Match DNATed packet.</td></tr><tr><td><i>disable</i></td><td>Do not match DNATed packet.</td></tr></table>	Option	Description	<i>enable</i>	Match DNATed packet.	<i>disable</i>	Do not match DNATed packet.					
Option	Description											
<i>enable</i>	Match DNATed packet.											
<i>disable</i>	Do not match DNATed packet.											
match-vip-only	Enable/disable matching of only those packets that have had their destination addresses changed by a VIP.	option	-	disable								

Parameter	Description	Type	Size	Default
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Enable matching of only those packets that have had their destination addresses changed by a VIP.		
	<i>disable</i>	Disable matching of only those packets that have had their destination addresses changed by a VIP.		
name	Policy name.	string	Maximum length: 35	
nat	Enable/disable source NAT.	option	-	disable
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
nat46	Enable/disable NAT46.	option	-	disable
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Enable NAT46.		
	<i>disable</i>	Disable NAT46.		
nat64	Enable/disable NAT64.	option	-	disable
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Enable NAT64.		
	<i>disable</i>	Disable NAT64.		
natinbound	Policy-based IPsec VPN: apply destination NAT to inbound traffic.	option	-	disable
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
natip	Policy-based IPsec VPN: source NAT IP address for outgoing traffic.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0
natoutbound	Policy-based IPsec VPN: apply source NAT to outbound traffic.	option	-	disable

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
np-acceleration *	Enable/disable UTM Network Processor acceleration.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable UTM Network Processor acceleration.		
	<i>disable</i>	Disable UTM Network Processor acceleration.		
ntlm	Enable/disable NTLM authentication.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
ntlm-enabled-browsers <user-agent-string>	HTTP-User-Agent value of supported browsers. User agent string.	string	Maximum length: 79	
ntlm-guest	Enable/disable NTLM guest user access.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
outbound	Policy-based IPsec VPN: only traffic from the internal network can initiate a VPN.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
passive-wan-health-measurement	Enable/disable passive WAN health measurement. When enabled, auto-asic-offload is disabled.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable Passive WAN health measurement.		

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable Passive WAN health measurement.</td></tr></table>	Option	Description	<i>disable</i>	Disable Passive WAN health measurement.					
	Option	Description								
<i>disable</i>	Disable Passive WAN health measurement.									
per-ip-shaper	Per-IP traffic shaper.	string	Maximum length: 35							
permit-any-host	Accept UDP packets from any host.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
	Option	Description								
	<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.									
permit-stun-host	Accept UDP packets from any Session Traversal Utilities for NAT (STUN) host.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
	Option	Description								
	<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.									
pfc-profile *	PFCP profile.	string	Maximum length: 63							
policy-offload *	Enable/Disable hardware session setup for CGNAT.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable policy offloading.</td></tr><tr><td><i>disable</i></td><td>Disable policy offloading.</td></tr></table>	Option	Description	<i>enable</i>	Enable policy offloading.	<i>disable</i>	Disable policy offloading.			
	Option	Description								
	<i>enable</i>	Enable policy offloading.								
<i>disable</i>	Disable policy offloading.									
policyid	Policy ID.	integer	Minimum value: 0 Maximum value: 4294967294	0						
poolname <name>	IP Pool names. IP pool name.	string	Maximum length: 79							
poolname6 <name>	IPv6 pool names. IPv6 pool name.	string	Maximum length: 79							
profile-group	Name of profile group.	string	Maximum length: 35							

Parameter	Description	Type	Size	Default						
profile-protocol-options	Name of an existing Protocol options profile.	string	Maximum length: 35	default						
profile-type	Determine whether the firewall policy allows security profile groups or single profiles only.	option	-	single						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>single</td><td>Do not allow security profile groups.</td></tr><tr><td>group</td><td>Allow security profile groups.</td></tr></table>	Option	Description	single	Do not allow security profile groups.	group	Allow security profile groups.			
Option	Description									
single	Do not allow security profile groups.									
group	Allow security profile groups.									
radius-mac-auth-bypass	Enable MAC authentication bypass. The bypassed MAC address must be received from RADIUS server.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable MAC authentication bypass.</td></tr><tr><td>disable</td><td>Disable MAC authentication bypass.</td></tr></table>	Option	Description	enable	Enable MAC authentication bypass.	disable	Disable MAC authentication bypass.			
Option	Description									
enable	Enable MAC authentication bypass.									
disable	Disable MAC authentication bypass.									
redirect-url	URL users are directed to after seeing and accepting the disclaimer or authenticating.	var-string	Maximum length: 1023							
replacemsg-override-group	Override the default replacement message group for this policy.	string	Maximum length: 35							
reputation-direction	Direction of the initial traffic for reputation to take effect.	option	-	destination						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>source</td><td>Check reputation for source address.</td></tr><tr><td>destination</td><td>Check reputation for destination address.</td></tr></table>	Option	Description	source	Check reputation for source address.	destination	Check reputation for destination address.			
Option	Description									
source	Check reputation for source address.									
destination	Check reputation for destination address.									
reputation-minimum	Minimum Reputation to take action.	integer	Minimum value: 0 Maximum value: 4294967295	0						
rtp-addr <name>	Address names if this is an RTP NAT policy. Address name.	string	Maximum length: 79							
rtp-nat	Enable Real Time Protocol (RTP) NAT.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable setting.</td></tr><tr><td>enable</td><td>Enable setting.</td></tr></table>	Option	Description	disable	Disable setting.	enable	Enable setting.			
Option	Description									
disable	Disable setting.									
enable	Enable setting.									



Parameter	Description	Type	Size	Default						
schedule	Schedule name.	string	Maximum length: 35							
schedule-timeout	Enable to force current sessions to end when the schedule object times out. Disable allows them to end from inactivity.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable schedule timeout.</td></tr><tr><td><i>disable</i></td><td>Disable schedule timeout.</td></tr></table>	Option	Description	<i>enable</i>	Enable schedule timeout.	<i>disable</i>	Disable schedule timeout.			
Option	Description									
<i>enable</i>	Enable schedule timeout.									
<i>disable</i>	Disable schedule timeout.									
sctp-filter-profile	Name of an existing SCTP filter profile.	string	Maximum length: 35							
send-deny-packet	Enable to send a reply when a session is denied or blocked by a firewall policy.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable deny-packet sending.</td></tr><tr><td><i>enable</i></td><td>Enable deny-packet sending.</td></tr></table>	Option	Description	<i>disable</i>	Disable deny-packet sending.	<i>enable</i>	Enable deny-packet sending.			
Option	Description									
<i>disable</i>	Disable deny-packet sending.									
<i>enable</i>	Enable deny-packet sending.									
service <name>	Service and service group names. Service and service group names.	string	Maximum length: 79							
service-negate	When enabled service specifies what the service must NOT be.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable negated service match.</td></tr><tr><td><i>disable</i></td><td>Disable negated service match.</td></tr></table>	Option	Description	<i>enable</i>	Enable negated service match.	<i>disable</i>	Disable negated service match.			
Option	Description									
<i>enable</i>	Enable negated service match.									
<i>disable</i>	Disable negated service match.									
session-ttl	TTL in seconds for sessions accepted by this policy.	user	Not Specified							
sgt <id>	Security group tags. Security group tag (1 - 65535).	integer	Minimum value: 1 Maximum value: 65535							
sgt-check	Enable/disable security group tags (SGT) check.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable SGT check.</td></tr><tr><td><i>disable</i></td><td>Disable SGT check.</td></tr></table>	Option	Description	<i>enable</i>	Enable SGT check.	<i>disable</i>	Disable SGT check.			
Option	Description									
<i>enable</i>	Enable SGT check.									
<i>disable</i>	Disable SGT check.									

Parameter	Description	Type	Size	Default						
src-vendor-mac <id>	Vendor MAC source ID. Vendor MAC ID.	integer	Minimum value: 0 Maximum value: 4294967295							
srcaddr <name>	Source IPv4 address and address group names. Address name.	string	Maximum length: 79							
srcaddr-negate	When enabled srcaddr/srcaddr6 specifies what the source address must NOT be.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable source address negate.</td></tr><tr><td>disable</td><td>Disable source address negate.</td></tr></table>				Option	Description	enable	Enable source address negate.	disable	Disable source address negate.
Option	Description									
enable	Enable source address negate.									
disable	Disable source address negate.									
srcaddr6 <name>	Source IPv6 address name and address group names. Address name.	string	Maximum length: 79							
srcintf <name>	Incoming (ingress) interface. Interface name.	string	Maximum length: 79							
ssh-filter-profile	Name of an existing SSH filter profile.	string	Maximum length: 35							
ssh-policy-redirect	Redirect SSH traffic to matching transparent proxy policy.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable SSH policy redirect.</td></tr><tr><td>disable</td><td>Disable SSH policy redirect.</td></tr></table>				Option	Description	enable	Enable SSH policy redirect.	disable	Disable SSH policy redirect.
Option	Description									
enable	Enable SSH policy redirect.									
disable	Disable SSH policy redirect.									
ssl-ssh-profile	Name of an existing SSL SSH profile.	string	Maximum length: 35	no-inspection						
status	Enable or disable this policy.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>				Option	Description	enable	Enable setting.	disable	Disable setting.
Option	Description									
enable	Enable setting.									
disable	Disable setting.									

Parameter	Description	Type	Size	Default								
tcp-mss-receiver	Receiver TCP maximum segment size (MSS).	integer	Minimum value: 0 Maximum value: 65535	0								
tcp-mss-sender	Sender TCP maximum segment size (MSS).	integer	Minimum value: 0 Maximum value: 65535	0								
tcp-session-without-syn	Enable/disable creation of TCP session without SYN flag.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>all</i></td><td>Enable TCP session without SYN.</td></tr><tr><td><i>data-only</i></td><td>Enable TCP session data only.</td></tr><tr><td><i>disable</i></td><td>Disable TCP session without SYN.</td></tr></table>				Option	Description	<i>all</i>	Enable TCP session without SYN.	<i>data-only</i>	Enable TCP session data only.	<i>disable</i>	Disable TCP session without SYN.
Option	Description											
<i>all</i>	Enable TCP session without SYN.											
<i>data-only</i>	Enable TCP session data only.											
<i>disable</i>	Disable TCP session without SYN.											
tcp-timeout-pid *	TCP timeout profile ID	integer	Minimum value: 0 Maximum value: 4294967295	0								
timeout-send-rst	Enable/disable sending RST packets when TCP sessions expire.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable sending of RST packet upon TCP session expiration.</td></tr><tr><td><i>disable</i></td><td>Disable sending of RST packet upon TCP session expiration.</td></tr></table>				Option	Description	<i>enable</i>	Enable sending of RST packet upon TCP session expiration.	<i>disable</i>	Disable sending of RST packet upon TCP session expiration.		
Option	Description											
<i>enable</i>	Enable sending of RST packet upon TCP session expiration.											
<i>disable</i>	Disable sending of RST packet upon TCP session expiration.											
tos	ToS (Type of Service) value used for comparison.	user	Not Specified									
tos-mask	Non-zero bit positions are used for comparison while zero bit positions are ignored.	user	Not Specified									
tos-negate	Enable negated TOS match.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable TOS match negate.</td></tr><tr><td><i>disable</i></td><td>Disable TOS match negate.</td></tr></table>				Option	Description	<i>enable</i>	Enable TOS match negate.	<i>disable</i>	Disable TOS match negate.		
Option	Description											
<i>enable</i>	Enable TOS match negate.											
<i>disable</i>	Disable TOS match negate.											
traffic-shaper	Traffic shaper.	string	Maximum length: 35									

Parameter	Description	Type	Size	Default						
traffic-shaper-reverse	Reverse traffic shaper.	string	Maximum length: 35							
udp-timeout-pid *	UDP timeout profile ID	integer	Minimum value: 0 Maximum value: 4294967295	0						
users <name>	Names of individual users that can authenticate with this policy. Names of individual users that can authenticate with this policy.	string	Maximum length: 79							
utm-status	Enable to add one or more security profiles (AV, IPS, etc.) to the firewall policy.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>	Option	Description	enable	Enable setting.	disable	Disable setting.			
Option	Description									
enable	Enable setting.									
disable	Disable setting.									
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000						
videofilter-profile	Name of an existing VideoFilter profile.	string	Maximum length: 35							
vlan-cos-fwd	VLAN forward direction user priority: 255 passthrough, 0 lowest, 7 highest.	integer	Minimum value: 0 Maximum value: 7	255						
vlan-cos-rev	VLAN reverse direction user priority: 255 passthrough, 0 lowest, 7 highest.	integer	Minimum value: 0 Maximum value: 7	255						
vlan-filter	Set VLAN filters.	user	Not Specified							
voip-profile	Name of an existing VoIP profile.	string	Maximum length: 35							
vpntunnel	Policy-based IPsec VPN: name of the IPsec VPN Phase 1.	string	Maximum length: 35							
waf-profile	Name of an existing Web application firewall profile.	string	Maximum length: 35							
wanopt *	Enable/disable WAN optimization.	option	-	disable						

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
wanopt-detection *	WAN optimization auto-detection mode.	option	-	active
	<b>Option</b>	<b>Description</b>		
	<i>active</i>	Active WAN optimization peer auto-detection.		
	<i>passive</i>	Passive WAN optimization peer auto-detection.		
	<i>off</i>	Turn off WAN optimization peer auto-detection.		
wanopt-passive-opt *	WAN optimization passive mode options. This option decides what IP address will be used to connect server.	option	-	default
	<b>Option</b>	<b>Description</b>		
	<i>default</i>	Allow client side WAN opt peer to decide.		
	<i>transparent</i>	Use address of client to connect to server.		
	<i>non-transparent</i>	Use local FortiGate address to connect to server.		
wanopt-peer *	WAN optimization peer.	string	Maximum length: 35	
wanopt-profile *	WAN optimization profile.	string	Maximum length: 35	
wccp	Enable/disable forwarding traffic matching this policy to a configured WCCP server.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable WCCP setting.		
	<i>disable</i>	Disable WCCP setting.		
webcache *	Enable/disable web cache.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

Parameter	Description	Type	Size	Default						
webcache-https *	Enable/disable web cache for HTTPS.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable web cache for HTTPS.</td></tr><tr><td><i>enable</i></td><td>Enable web cache for HTTPS.</td></tr></table>	Option	Description	<i>disable</i>	Disable web cache for HTTPS.	<i>enable</i>	Enable web cache for HTTPS.			
Option	Description									
<i>disable</i>	Disable web cache for HTTPS.									
<i>enable</i>	Enable web cache for HTTPS.									
webfilter-profile	Name of an existing Web filter profile.	string	Maximum length: 35							
webproxy-forward-server	Webproxy forward server name.	string	Maximum length: 63							
webproxy-profile	Webproxy profile name.	string	Maximum length: 63							
ztna-ems-tag <name>	Source ztna-ems-tag names. Address name.	string	Maximum length: 79							
ztna-geo-tag <name>	Source ztna-geo-tag names. Address name.	string	Maximum length: 79							
ztna-status	Enable/disable zero trust access.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable zero trust network access.</td></tr><tr><td><i>disable</i></td><td>Disable zero trust network access.</td></tr></table>	Option	Description	<i>enable</i>	Enable zero trust network access.	<i>disable</i>	Disable zero trust network access.			
Option	Description									
<i>enable</i>	Enable zero trust network access.									
<i>disable</i>	Disable zero trust network access.									

\* This parameter may not exist in some models.

## config firewall profile-group

Configure profile groups.

```
config firewall profile-group
  Description: Configure profile groups.
  edit <name>
    set application-list {string}
    set av-profile {string}
    set cifs-profile {string}
    set dlp-sensor {string}
    set dnsfilter-profile {string}
    set emailfilter-profile {string}
    set file-filter-profile {string}
    set icap-profile {string}
    set ips-sensor {string}
    set profile-protocol-options {string}
    set sctp-filter-profile {string}
    set ssh-filter-profile {string}
```

```

        set ssl-ssh-profile {string}
        set videofilter-profile {string}
        set voip-profile {string}
        set waf-profile {string}
        set webfilter-profile {string}
    next
end

```

## config firewall profile-group

Parameter	Description	Type	Size	Default
application-list	Name of an existing Application list.	string	Maximum length: 35	
av-profile	Name of an existing Antivirus profile.	string	Maximum length: 35	
cifs-profile	Name of an existing CIFS profile.	string	Maximum length: 35	
dlp-sensor	Name of an existing DLP sensor.	string	Maximum length: 35	
dnsfilter-profile	Name of an existing DNS filter profile.	string	Maximum length: 35	
emailfilter-profile	Name of an existing email filter profile.	string	Maximum length: 35	
file-filter-profile	Name of an existing file-filter profile.	string	Maximum length: 35	
icap-profile	Name of an existing ICAP profile.	string	Maximum length: 35	
ips-sensor	Name of an existing IPS sensor.	string	Maximum length: 35	
name	Profile group name.	string	Maximum length: 35	
profile-protocol-options	Name of an existing Protocol options profile.	string	Maximum length: 35	default
sctp-filter-profile	Name of an existing SCTP filter profile.	string	Maximum length: 35	
ssh-filter-profile	Name of an existing SSH filter profile.	string	Maximum length: 35	
ssl-ssh-profile	Name of an existing SSL SSH profile.	string	Maximum length: 35	certificate-inspection

Parameter	Description	Type	Size	Default
videofilter-profile	Name of an existing VideoFilter profile.	string	Maximum length: 35	
voip-profile	Name of an existing VoIP profile.	string	Maximum length: 35	
waf-profile	Name of an existing Web application firewall profile.	string	Maximum length: 35	
webfilter-profile	Name of an existing Web filter profile.	string	Maximum length: 35	

## config firewall profile-protocol-options

Configure protocol options.

```
config firewall profile-protocol-options
    Description: Configure protocol options.
    edit <name>
        config cifs
            Description: Configure CIFS protocol options.
            set ports {integer}
            set status [enable|disable]
            set options {option1}, {option2}, ...
            set oversize-limit {integer}
            set uncompressed-oversize-limit {integer}
            set uncompressed-nest-limit {integer}
            set scan-bzip2 [enable|disable]
            set tcp-window-type [auto-tuning|system|...]
            set tcp-window-minimum {integer}
            set tcp-window-maximum {integer}
            set tcp-window-size {integer}
            set server-credential-type [none|credential-replication|...]
            set domain-controller {string}
        config server-keytab
            Description: Server keytab.
            edit <principal>
                set keytab {string}
            next
        end
    end
    set comment {var-string}
    config dns
        Description: Configure DNS protocol options.
        set ports {integer}
        set status [enable|disable]
    end
    config ftp
        Description: Configure FTP protocol options.
        set ports {integer}
        set status [enable|disable]
        set inspect-all [enable|disable]
        set options {option1}, {option2}, ...
```



```

    set comfort-interval {integer}
    set comfort-amount {integer}
    set oversize-limit {integer}
    set uncompressed-oversize-limit {integer}
    set uncompressed-nest-limit {integer}
    set stream-based-uncompressed-limit {integer}
    set scan-bzip2 [enable|disable]
    set tcp-window-type [auto-tuning|system|...]
    set tcp-window-minimum {integer}
    set tcp-window-maximum {integer}
    set tcp-window-size {integer}
    set ssl-offloaded [no|yes]
    set explicit-ftp-tls [enable|disable]
end
config http
    Description: Configure HTTP protocol options.
    set ports {integer}
    set status [enable|disable]
    set inspect-all [enable|disable]
    set proxy-after-tcp-handshake [enable|disable]
    set options {option1}, {option2}, ...
    set comfort-interval {integer}
    set comfort-amount {integer}
    set range-block [disable|enable]
    set strip-x-forwarded-for [disable|enable]
    set post-lang {option1}, {option2}, ...
    set streaming-content-bypass [enable|disable]
    set switching-protocols [bypass|block]
    set unknown-http-version [reject|tunnel|...]
    set tunnel-non-http [enable|disable]
    set oversize-limit {integer}
    set uncompressed-oversize-limit {integer}
    set uncompressed-nest-limit {integer}
    set stream-based-uncompressed-limit {integer}
    set scan-bzip2 [enable|disable]
    set block-page-status-code {integer}
    set retry-count {integer}
    set tcp-window-type [auto-tuning|system|...]
    set tcp-window-minimum {integer}
    set tcp-window-maximum {integer}
    set tcp-window-size {integer}
    set ssl-offloaded [no|yes]
    set address-ip-rating [enable|disable]
end
config imap
    Description: Configure IMAP protocol options.
    set ports {integer}
    set status [enable|disable]
    set inspect-all [enable|disable]
    set proxy-after-tcp-handshake [enable|disable]
    set options {option1}, {option2}, ...
    set oversize-limit {integer}
    set uncompressed-oversize-limit {integer}
    set uncompressed-nest-limit {integer}
    set scan-bzip2 [enable|disable]
    set ssl-offloaded [no|yes]

```

```

end
config mail-signature
    Description: Configure Mail signature.
    set status [disable|enable]
    set signature {string}
end
config mapi
    Description: Configure MAPI protocol options.
    set ports {integer}
    set status [enable|disable]
    set options {option1}, {option2}, ...
    set oversize-limit {integer}
    set uncompressed-oversize-limit {integer}
    set uncompressed-nest-limit {integer}
    set scan-bzip2 [enable|disable]
end
config nntp
    Description: Configure NNTP protocol options.
    set ports {integer}
    set status [enable|disable]
    set inspect-all [enable|disable]
    set proxy-after-tcp-handshake [enable|disable]
    set options {option1}, {option2}, ...
    set oversize-limit {integer}
    set uncompressed-oversize-limit {integer}
    set uncompressed-nest-limit {integer}
    set scan-bzip2 [enable|disable]
end
set oversize-log [disable|enable]
config pop3
    Description: Configure POP3 protocol options.
    set ports {integer}
    set status [enable|disable]
    set inspect-all [enable|disable]
    set proxy-after-tcp-handshake [enable|disable]
    set options {option1}, {option2}, ...
    set oversize-limit {integer}
    set uncompressed-oversize-limit {integer}
    set uncompressed-nest-limit {integer}
    set scan-bzip2 [enable|disable]
    set ssl-offloaded [no|yes]
end
set replacemsg-group {string}
set rpc-over-http [enable|disable]
config smtp
    Description: Configure SMTP protocol options.
    set ports {integer}
    set status [enable|disable]
    set inspect-all [enable|disable]
    set proxy-after-tcp-handshake [enable|disable]
    set options {option1}, {option2}, ...
    set oversize-limit {integer}
    set uncompressed-oversize-limit {integer}
    set uncompressed-nest-limit {integer}
    set scan-bzip2 [enable|disable]
    set server-busy [enable|disable]

```

```

        set ssl-offloaded [no|yes]
    end
    config ssh
        Description: Configure SFTP and SCP protocol options.
        set options {option1}, {option2}, ...
        set comfort-interval {integer}
        set comfort-amount {integer}
        set oversize-limit {integer}
        set uncompressed-oversize-limit {integer}
        set uncompressed-nest-limit {integer}
        set stream-based-uncompressed-limit {integer}
        set scan-bzip2 [enable|disable]
        set tcp-window-type [auto-tuning|system|...]
        set tcp-window-minimum {integer}
        set tcp-window-maximum {integer}
        set tcp-window-size {integer}
        set ssl-offloaded [no|yes]
    end
    set switching-protocols-log [disable|enable]
next
end

```

## config firewall profile-protocol-options

Parameter	Description	Type	Size	Default						
comment	Optional comments.	var-string	Maximum length: 255							
name	Name.	string	Maximum length: 35							
oversize-log	Enable/disable logging for antivirus oversize file blocking.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable logging for antivirus oversize file blocking.</td></tr><tr><td><i>enable</i></td><td>Enable logging for antivirus oversize file blocking.</td></tr></table>	Option	Description	<i>disable</i>	Disable logging for antivirus oversize file blocking.	<i>enable</i>	Enable logging for antivirus oversize file blocking.			
Option	Description									
<i>disable</i>	Disable logging for antivirus oversize file blocking.									
<i>enable</i>	Enable logging for antivirus oversize file blocking.									
replacemsg-group	Name of the replacement message group to be used.	string	Maximum length: 35							
rpc-over-http	Enable/disable inspection of RPC over HTTP.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable inspection of RPC over HTTP.</td></tr><tr><td><i>disable</i></td><td>Disable inspection of RPC over HTTP.</td></tr></table>	Option	Description	<i>enable</i>	Enable inspection of RPC over HTTP.	<i>disable</i>	Disable inspection of RPC over HTTP.			
Option	Description									
<i>enable</i>	Enable inspection of RPC over HTTP.									
<i>disable</i>	Disable inspection of RPC over HTTP.									
switching-protocols-log	Enable/disable logging for HTTP/HTTPS switching protocols.	option	-	disable						

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable logging for HTTP/HTTPS switching protocols.		
	<i>enable</i>	Enable logging for HTTP/HTTPS switching protocols.		

## config cifs

Parameter	Description	Type	Size	Default
ports	Ports to scan for content.	integer	Minimum value: 1 Maximum value: 65535	
status	Enable/disable the active status of scanning for this protocol.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
options	One or more options that can be applied to the session.	option	-	
	<b>Option</b>	<b>Description</b>		
	<i>oversize</i>	Block oversized file.		
oversize-limit	Maximum in-memory file size that can be scanned.	integer	Minimum value: 1 Maximum value: 1606 **	10
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned.	integer	Minimum value: 1 Maximum value: 1606 **	10
uncompressed-nest-limit	Maximum nested levels of compression that can be uncompressed and scanned.	integer	Minimum value: 2 Maximum value: 100	12
scan-bzip2	Enable/disable scanning of BZip2 compressed files.	option	-	enable

Parameter	Description	Type	Size	Default										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.							
	Option	Description												
	<i>enable</i>	Enable setting.												
<i>disable</i>	Disable setting.													
tcp-window-type	TCP window type to use for this protocol.	option	-	auto-tuning										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto-tuning</i></td><td>Allow system to auto-tune TCP window size (default).</td></tr><tr><td><i>system</i></td><td>Use system default TCP window size for this protocol.</td></tr><tr><td><i>static</i></td><td>Manually specify TCP window size.</td></tr><tr><td><i>dynamic</i></td><td>Vary TCP window size based on available memory and within limits of tcp-window-minimum and tcp-window-maximum.</td></tr></table>	Option	Description	<i>auto-tuning</i>	Allow system to auto-tune TCP window size (default).	<i>system</i>	Use system default TCP window size for this protocol.	<i>static</i>	Manually specify TCP window size.	<i>dynamic</i>	Vary TCP window size based on available memory and within limits of tcp-window-minimum and tcp-window-maximum.			
	Option	Description												
	<i>auto-tuning</i>	Allow system to auto-tune TCP window size (default).												
	<i>system</i>	Use system default TCP window size for this protocol.												
	<i>static</i>	Manually specify TCP window size.												
<i>dynamic</i>	Vary TCP window size based on available memory and within limits of tcp-window-minimum and tcp-window-maximum.													
tcp-window-minimum	Minimum dynamic TCP window size.	integer	Minimum value: 65536 Maximum value: 1048576	131072										
tcp-window-maximum	Maximum dynamic TCP window size.	integer	Minimum value: 1048576 Maximum value: 33554432	8388608										
tcp-window-size	Set TCP static window size.	integer	Minimum value: 65536 Maximum value: 33554432	262144										
server-credential-type	CIFS server credential type.	option	-	none										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>Credential derivation not set.</td></tr><tr><td><i>credential-replication</i></td><td>Credential derived using Replication account on Domain Controller.</td></tr><tr><td><i>credential-keytab</i></td><td>Credential derived using server keytab.</td></tr></table>	Option	Description	<i>none</i>	Credential derivation not set.	<i>credential-replication</i>	Credential derived using Replication account on Domain Controller.	<i>credential-keytab</i>	Credential derived using server keytab.					
	Option	Description												
	<i>none</i>	Credential derivation not set.												
	<i>credential-replication</i>	Credential derived using Replication account on Domain Controller.												
<i>credential-keytab</i>	Credential derived using server keytab.													

Parameter	Description	Type	Size	Default
domain-controller	Domain for which to decrypt CIFS traffic.	string	Maximum length: 63	

\*\* Values may differ between models.

#### config server-keytab

Parameter	Description	Type	Size	Default
principal	Service principal. For example, host/cifsserver.example.com@example.com.	string	Maximum length: 511	
keytab	Base64 encoded keytab file containing credential of the server.	string	Maximum length: 8191	

#### config dns

Parameter	Description	Type	Size	Default
ports	Ports to scan for content.	integer	Minimum value: 1 Maximum value: 65535	
status	Enable/disable the active status of scanning for this protocol.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

#### config ftp

Parameter	Description	Type	Size	Default
ports	Ports to scan for content.	integer	Minimum value: 1 Maximum value: 65535	
status	Enable/disable the active status of scanning for this protocol.	option	-	enable

Parameter	Description	Type	Size	Default												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.									
	Option	Description														
	<i>enable</i>	Enable setting.														
<i>disable</i>	Disable setting.															
inspect-all	Enable/disable the inspection of all ports for the protocol.	option	-	disable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.									
	Option	Description														
	<i>enable</i>	Enable setting.														
<i>disable</i>	Disable setting.															
options	One or more options that can be applied to the session.	option	-													
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>clientcomfort</i></td><td>Prevent client timeout.</td></tr><tr><td><i>oversize</i></td><td>Block oversized file.</td></tr><tr><td><i>splice</i></td><td>Enable splice mode.</td></tr><tr><td><i>bypass-rest-command</i></td><td>Bypass REST command.</td></tr><tr><td><i>bypass-mode-command</i></td><td>Bypass MODE command.</td></tr></table>	Option	Description	<i>clientcomfort</i>	Prevent client timeout.	<i>oversize</i>	Block oversized file.	<i>splice</i>	Enable splice mode.	<i>bypass-rest-command</i>	Bypass REST command.	<i>bypass-mode-command</i>	Bypass MODE command.			
	Option	Description														
	<i>clientcomfort</i>	Prevent client timeout.														
	<i>oversize</i>	Block oversized file.														
	<i>splice</i>	Enable splice mode.														
	<i>bypass-rest-command</i>	Bypass REST command.														
<i>bypass-mode-command</i>	Bypass MODE command.															
comfort-interval	Period of time between start, or last transmission, and the next client comfort transmission of data.	integer	Minimum value: 1 Maximum value: 900	10												
comfort-amount	Amount of data to send in a transmission for client comforting.	integer	Minimum value: 1 Maximum value: 65535	1												
oversize-limit	Maximum in-memory file size that can be scanned.	integer	Minimum value: 1 Maximum value: 1606 **	10												
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned.	integer	Minimum value: 1 Maximum value: 1606 **	10												

Parameter	Description	Type	Size	Default										
uncompressed-nest-limit	Maximum nested levels of compression that can be uncompressed and scanned.	integer	Minimum value: 2 Maximum value: 100	12										
stream-based-uncompressed-limit	Maximum stream-based uncompressed data size that will be scanned in megabytes. Stream-based uncompression used only under certain conditions.	integer	Minimum value: 0 Maximum value: 4294967295	0										
scan-bzip2	Enable/disable scanning of BZip2 compressed files.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>				Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.				
	Option	Description												
	<i>enable</i>	Enable setting.												
<i>disable</i>	Disable setting.													
tcp-window-type	TCP window type to use for this protocol.	option	-	auto-tuning										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto-tuning</i></td><td>Allow system to auto-tune TCP window size (default).</td></tr><tr><td><i>system</i></td><td>Use system default TCP window size for this protocol.</td></tr><tr><td><i>static</i></td><td>Manually specify TCP window size.</td></tr><tr><td><i>dynamic</i></td><td>Vary TCP window size based on available memory and within limits of tcp-window-minimum and tcp-window-maximum.</td></tr></table>				Option	Description	<i>auto-tuning</i>	Allow system to auto-tune TCP window size (default).	<i>system</i>	Use system default TCP window size for this protocol.	<i>static</i>	Manually specify TCP window size.	<i>dynamic</i>	Vary TCP window size based on available memory and within limits of tcp-window-minimum and tcp-window-maximum.
	Option	Description												
	<i>auto-tuning</i>	Allow system to auto-tune TCP window size (default).												
	<i>system</i>	Use system default TCP window size for this protocol.												
	<i>static</i>	Manually specify TCP window size.												
<i>dynamic</i>	Vary TCP window size based on available memory and within limits of tcp-window-minimum and tcp-window-maximum.													
tcp-window-minimum	Minimum dynamic TCP window size.	integer	Minimum value: 65536 Maximum value: 1048576	131072										
tcp-window-maximum	Maximum dynamic TCP window size.	integer	Minimum value: 1048576 Maximum value: 33554432	8388608										
tcp-window-size	Set TCP static window size.	integer	Minimum value: 65536 Maximum value: 33554432	262144										



Parameter	Description	Type	Size	Default
ssl-offloaded	SSL decryption and encryption performed by an external device.	option	-	no
	<b>Option</b>	<b>Description</b>		
	<i>no</i>	SSL decryption and encryption performed by FortiGate when deep-inspection is enabled.		
	<i>yes</i>	SSL decryption and encryption performed by an external device.		
explicit-ftp-tls	Enable/disable FTP redirection for explicit FTPS.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

\*\* Values may differ between models.

## config http

Parameter	Description	Type	Size	Default
ports	Ports to scan for content.	integer	Minimum value: 1 Maximum value: 65535	
status	Enable/disable the active status of scanning for this protocol.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
inspect-all	Enable/disable the inspection of all ports for the protocol.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
proxy-after-tcp-handshake	Proxy traffic after the TCP 3-way handshake has been established (not before).	option	-	disable

Parameter	Description	Type	Size	Default										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.							
	Option	Description												
	<i>enable</i>	Enable setting.												
<i>disable</i>	Disable setting.													
options	One or more options that can be applied to the session.	option	-											
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>clientcomfort</i></td><td>Prevent client timeout.</td></tr><tr><td><i>servercomfort</i></td><td>Prevent server timeout.</td></tr><tr><td><i>oversize</i></td><td>Block oversized file.</td></tr><tr><td><i>chunkedbypass</i></td><td>Bypass chunked transfer encoded sites.</td></tr></table>	Option	Description	<i>clientcomfort</i>	Prevent client timeout.	<i>servercomfort</i>	Prevent server timeout.	<i>oversize</i>	Block oversized file.	<i>chunkedbypass</i>	Bypass chunked transfer encoded sites.			
	Option	Description												
	<i>clientcomfort</i>	Prevent client timeout.												
	<i>servercomfort</i>	Prevent server timeout.												
	<i>oversize</i>	Block oversized file.												
<i>chunkedbypass</i>	Bypass chunked transfer encoded sites.													
comfort-interval	Period of time between start, or last transmission, and the next client comfort transmission of data.	integer	Minimum value: 1 Maximum value: 900	10										
comfort-amount	Amount of data to send in a transmission for client comforting.	integer	Minimum value: 1 Maximum value: 65535	1										
range-block	Enable/disable blocking of partial downloads.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable range header blocking (allow partial file downloads)</td></tr><tr><td><i>enable</i></td><td>Enable range header blocking (treat all partial file downloads as full file download)</td></tr></table>	Option	Description	<i>disable</i>	Disable range header blocking (allow partial file downloads)	<i>enable</i>	Enable range header blocking (treat all partial file downloads as full file download)							
	Option	Description												
	<i>disable</i>	Disable range header blocking (allow partial file downloads)												
<i>enable</i>	Enable range header blocking (treat all partial file downloads as full file download)													
strip-x-forwarded-for	Enable/disable stripping of HTTP X-Forwarded-For header.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable changing of HTTP X-Forwarded-For header.</td></tr><tr><td><i>enable</i></td><td>Enable replacement of X-Forwarded-For value with 1.1.1.1.</td></tr></table>	Option	Description	<i>disable</i>	Disable changing of HTTP X-Forwarded-For header.	<i>enable</i>	Enable replacement of X-Forwarded-For value with 1.1.1.1.							
	Option	Description												
	<i>disable</i>	Disable changing of HTTP X-Forwarded-For header.												
<i>enable</i>	Enable replacement of X-Forwarded-For value with 1.1.1.1.													
post-lang	ID codes for character sets to be used to convert to UTF-8 for banned words and DLP on HTTP posts (maximum of 5 character sets).	option	-											

Parameter	Description	Type	Size	Default																																													
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>jisx0201</i></td><td>Japanese Industrial Standard 0201.</td></tr><tr><td><i>jisx0208</i></td><td>Japanese Industrial Standard 0208.</td></tr><tr><td><i>jisx0212</i></td><td>Japanese Industrial Standard 0212.</td></tr><tr><td><i>gb2312</i></td><td>Guojia Biaozhun 2312 (simplified Chinese).</td></tr><tr><td><i>ksc5601-ex</i></td><td>Wansung Korean standard 5601.</td></tr><tr><td><i>euc-jp</i></td><td>Extended Unicode Japanese.</td></tr><tr><td><i>sjis</i></td><td>Shift Japanese Industrial Standard.</td></tr><tr><td><i>iso2022-jp</i></td><td>ISO 2022 Japanese.</td></tr><tr><td><i>iso2022-jp-1</i></td><td>ISO 2022-1 Japanese.</td></tr><tr><td><i>iso2022-jp-2</i></td><td>ISO 2022-2 Japanese.</td></tr><tr><td><i>euc-cn</i></td><td>Extended Unicode Chinese.</td></tr><tr><td><i>ces-gbk</i></td><td>Extended GB2312 (simplified Chinese).</td></tr><tr><td><i>hz</i></td><td>Hanzi simplified Chinese.</td></tr><tr><td><i>ces-big5</i></td><td>Big-5 traditional Chinese.</td></tr><tr><td><i>euc-kr</i></td><td>Extended Unicode Korean.</td></tr><tr><td><i>iso2022-jp-3</i></td><td>ISO 2022-3 Japanese.</td></tr><tr><td><i>iso8859-1</i></td><td>ISO 8859 Part 1 (Western European).</td></tr><tr><td><i>tis620</i></td><td>Thai Industrial Standard 620.</td></tr><tr><td><i>cp874</i></td><td>Code Page 874 (Thai).</td></tr><tr><td><i>cp1252</i></td><td>Code Page 1252 (Western European Latin).</td></tr><tr><td><i>cp1251</i></td><td>Code Page 1251 (Cyrillic).</td></tr></table>	Option	Description	<i>jisx0201</i>	Japanese Industrial Standard 0201.	<i>jisx0208</i>	Japanese Industrial Standard 0208.	<i>jisx0212</i>	Japanese Industrial Standard 0212.	<i>gb2312</i>	Guojia Biaozhun 2312 (simplified Chinese).	<i>ksc5601-ex</i>	Wansung Korean standard 5601.	<i>euc-jp</i>	Extended Unicode Japanese.	<i>sjis</i>	Shift Japanese Industrial Standard.	<i>iso2022-jp</i>	ISO 2022 Japanese.	<i>iso2022-jp-1</i>	ISO 2022-1 Japanese.	<i>iso2022-jp-2</i>	ISO 2022-2 Japanese.	<i>euc-cn</i>	Extended Unicode Chinese.	<i>ces-gbk</i>	Extended GB2312 (simplified Chinese).	<i>hz</i>	Hanzi simplified Chinese.	<i>ces-big5</i>	Big-5 traditional Chinese.	<i>euc-kr</i>	Extended Unicode Korean.	<i>iso2022-jp-3</i>	ISO 2022-3 Japanese.	<i>iso8859-1</i>	ISO 8859 Part 1 (Western European).	<i>tis620</i>	Thai Industrial Standard 620.	<i>cp874</i>	Code Page 874 (Thai).	<i>cp1252</i>	Code Page 1252 (Western European Latin).	<i>cp1251</i>	Code Page 1251 (Cyrillic).				
	Option	Description																																															
	<i>jisx0201</i>	Japanese Industrial Standard 0201.																																															
	<i>jisx0208</i>	Japanese Industrial Standard 0208.																																															
	<i>jisx0212</i>	Japanese Industrial Standard 0212.																																															
	<i>gb2312</i>	Guojia Biaozhun 2312 (simplified Chinese).																																															
	<i>ksc5601-ex</i>	Wansung Korean standard 5601.																																															
	<i>euc-jp</i>	Extended Unicode Japanese.																																															
	<i>sjis</i>	Shift Japanese Industrial Standard.																																															
	<i>iso2022-jp</i>	ISO 2022 Japanese.																																															
	<i>iso2022-jp-1</i>	ISO 2022-1 Japanese.																																															
	<i>iso2022-jp-2</i>	ISO 2022-2 Japanese.																																															
	<i>euc-cn</i>	Extended Unicode Chinese.																																															
	<i>ces-gbk</i>	Extended GB2312 (simplified Chinese).																																															
	<i>hz</i>	Hanzi simplified Chinese.																																															
	<i>ces-big5</i>	Big-5 traditional Chinese.																																															
	<i>euc-kr</i>	Extended Unicode Korean.																																															
	<i>iso2022-jp-3</i>	ISO 2022-3 Japanese.																																															
	<i>iso8859-1</i>	ISO 8859 Part 1 (Western European).																																															
	<i>tis620</i>	Thai Industrial Standard 620.																																															
<i>cp874</i>	Code Page 874 (Thai).																																																
<i>cp1252</i>	Code Page 1252 (Western European Latin).																																																
<i>cp1251</i>	Code Page 1251 (Cyrillic).																																																
streaming-content-bypass	Enable/disable bypassing of streaming content from buffering.	option	-	enable																																													
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.																																										
	Option	Description																																															
	<i>enable</i>	Enable setting.																																															
<i>disable</i>	Disable setting.																																																
switching-protocols	Bypass from scanning, or block a connection that attempts to switch protocol.	option	-	bypass																																													

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>bypass</td><td>Bypass connections when switching protocols.</td></tr><tr><td>block</td><td>Block connections when switching protocols.</td></tr></table>	Option	Description	bypass	Bypass connections when switching protocols.	block	Block connections when switching protocols.					
	Option	Description										
	bypass	Bypass connections when switching protocols.										
block	Block connections when switching protocols.											
unknown-http-version	How to handle HTTP sessions that do not comply with HTTP 0.9, 1.0, or 1.1.	option	-	reject								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>reject</td><td>Reject or tear down HTTP sessions that do not use HTTP 0.9, 1.0, or 1.1.</td></tr><tr><td>tunnel</td><td>Pass HTTP traffic that does not use HTTP 0.9, 1.0, or 1.1 without applying HTTP protocol optimization, byte-caching, or web caching. TCP protocol optimization is applied.</td></tr><tr><td>best-effort</td><td>Assume all HTTP sessions comply with HTTP 0.9, 1.0, or 1.1. If a session uses a different HTTP version, it may not parse correctly and the connection may be lost.</td></tr></table>	Option	Description	reject	Reject or tear down HTTP sessions that do not use HTTP 0.9, 1.0, or 1.1.	tunnel	Pass HTTP traffic that does not use HTTP 0.9, 1.0, or 1.1 without applying HTTP protocol optimization, byte-caching, or web caching. TCP protocol optimization is applied.	best-effort	Assume all HTTP sessions comply with HTTP 0.9, 1.0, or 1.1. If a session uses a different HTTP version, it may not parse correctly and the connection may be lost.			
	Option	Description										
	reject	Reject or tear down HTTP sessions that do not use HTTP 0.9, 1.0, or 1.1.										
	tunnel	Pass HTTP traffic that does not use HTTP 0.9, 1.0, or 1.1 without applying HTTP protocol optimization, byte-caching, or web caching. TCP protocol optimization is applied.										
best-effort	Assume all HTTP sessions comply with HTTP 0.9, 1.0, or 1.1. If a session uses a different HTTP version, it may not parse correctly and the connection may be lost.											
tunnel-non-http	Configure how to process non-HTTP traffic when a profile configured for HTTP traffic accepts a non-HTTP session. Can occur if an application sends non-HTTP traffic using an HTTP destination port.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Pass non-HTTP sessions through the tunnel without applying protocol optimization, byte-caching, or web caching. TCP protocol optimization is applied.</td></tr><tr><td>disable</td><td>Drop or tear down non-HTTP sessions accepted by the profile.</td></tr></table>	Option	Description	enable	Pass non-HTTP sessions through the tunnel without applying protocol optimization, byte-caching, or web caching. TCP protocol optimization is applied.	disable	Drop or tear down non-HTTP sessions accepted by the profile.					
	Option	Description										
	enable	Pass non-HTTP sessions through the tunnel without applying protocol optimization, byte-caching, or web caching. TCP protocol optimization is applied.										
disable	Drop or tear down non-HTTP sessions accepted by the profile.											
oversize-limit	Maximum in-memory file size that can be scanned.	integer	Minimum value: 1 Maximum value: 1606 **	10								
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned.	integer	Minimum value: 1 Maximum value: 1606 **	10								
uncompressed-nest-limit	Maximum nested levels of compression that can be uncompressed and scanned.	integer	Minimum value: 2 Maximum value: 100	12								

Parameter	Description	Type	Size	Default
stream-based-uncompressed-limit	Maximum stream-based uncompressed data size that will be scanned in megabytes. Stream-based uncompression used only under certain conditions.	integer	Minimum value: 0 Maximum value: 4294967295	0
scan-bzip2	Enable/disable scanning of BZip2 compressed files.	option	-	enable
	Option	Description		
	enable	Enable setting.		
	disable	Disable setting.		
block-page-status-code	Code number returned for blocked HTTP pages.	integer	Minimum value: 100 Maximum value: 599	403
retry-count	Number of attempts to retry HTTP connection.	integer	Minimum value: 0 Maximum value: 100	0
tcp-window-type	TCP window type to use for this protocol.	option	-	auto-tuning
	Option	Description		
	auto-tuning	Allow system to auto-tune TCP window size (default).		
	system	Use system default TCP window size for this protocol.		
	static	Manually specify TCP window size.		
	dynamic	Vary TCP window size based on available memory and within limits of tcp-window-minimum and tcp-window-maximum.		
tcp-window-minimum	Minimum dynamic TCP window size.	integer	Minimum value: 65536 Maximum value: 1048576	131072
tcp-window-maximum	Maximum dynamic TCP window size.	integer	Minimum value: 1048576 Maximum value: 33554432	8388608

Parameter	Description	Type	Size	Default						
tcp-window-size	Set TCP static window size.	integer	Minimum value: 65536 Maximum value: 33554432	262144						
ssl-offloaded	SSL decryption and encryption performed by an external device.	option	-	no						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>no</td><td>SSL decryption and encryption performed by FortiGate when deep-inspection is enabled.</td></tr><tr><td>yes</td><td>SSL decryption and encryption performed by an external device.</td></tr></table>				Option	Description	no	SSL decryption and encryption performed by FortiGate when deep-inspection is enabled.	yes	SSL decryption and encryption performed by an external device.
	Option	Description								
	no	SSL decryption and encryption performed by FortiGate when deep-inspection is enabled.								
yes	SSL decryption and encryption performed by an external device.									
address-ip-rating	Enable/disable IP based URL rating.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>				Option	Description	enable	Enable setting.	disable	Disable setting.
	Option	Description								
	enable	Enable setting.								
disable	Disable setting.									

\*\* Values may differ between models.

## config imap

Parameter	Description	Type	Size	Default						
ports	Ports to scan for content.	integer	Minimum value: 1 Maximum value: 65535							
status	Enable/disable the active status of scanning for this protocol.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>				Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.
	Option	Description								
	<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.									
inspect-all	Enable/disable the inspection of all ports for the protocol.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr></table>				Option	Description	<i>enable</i>	Enable setting.		
	Option	Description								
<i>enable</i>	Enable setting.									

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>disable</i>	Disable setting.					
	Option	Description								
	<i>disable</i>	Disable setting.								
proxy-after-tcp-handshake	Proxy traffic after the TCP 3-way handshake has been established (not before).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
	Option	Description								
	<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.									
options	One or more options that can be applied to the session.	option	-							
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>fragmail</i></td><td>Pass fragmented email.</td></tr><tr><td><i>oversize</i></td><td>Block oversized email.</td></tr></table>	Option	Description	<i>fragmail</i>	Pass fragmented email.	<i>oversize</i>	Block oversized email.			
	Option	Description								
	<i>fragmail</i>	Pass fragmented email.								
<i>oversize</i>	Block oversized email.									
oversize-limit	Maximum in-memory file size that can be scanned.	integer	Minimum value: 1 Maximum value: 1606 **	10						
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned.	integer	Minimum value: 1 Maximum value: 1606 **	10						
uncompressed-nest-limit	Maximum nested levels of compression that can be uncompressed and scanned.	integer	Minimum value: 2 Maximum value: 100	12						
scan-bzip2	Enable/disable scanning of BZip2 compressed files.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
	Option	Description								
	<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.									
ssl-offloaded	SSL decryption and encryption performed by an external device.	option	-	no						

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>no</i>	SSL decryption and encryption performed by FortiGate when deep-inspection is enabled.		
	<i>yes</i>	SSL decryption and encryption performed by an external device.		

\*\* Values may differ between models.

### config mail-signature

Parameter	Description	Type	Size	Default
status	Enable/disable adding an email signature to SMTP email messages as they pass through the FortiGate.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable mail signature.		
	<i>enable</i>	Enable mail signature.		
signature	Email signature to be added to outgoing email (if the signature contains spaces, enclose with quotation marks).	string	Maximum length: 1023	

### config mapi

Parameter	Description	Type	Size	Default
ports	Ports to scan for content.	integer	Minimum value: 1 Maximum value: 65535	
status	Enable/disable the active status of scanning for this protocol.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
options	One or more options that can be applied to the session.	option	-	



Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>fragmail</i>	Pass fragmented email.		
	<i>oversize</i>	Block oversized email.		
oversize-limit	Maximum in-memory file size that can be scanned.	integer	Minimum value: 1 Maximum value: 1606 **	10
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned.	integer	Minimum value: 1 Maximum value: 1606 **	10
uncompressed-nest-limit	Maximum nested levels of compression that can be uncompressed and scanned.	integer	Minimum value: 2 Maximum value: 100	12
scan-bzip2	Enable/disable scanning of BZip2 compressed files.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

\*\* Values may differ between models.

## config nntp

Parameter	Description	Type	Size	Default
ports	Ports to scan for content.	integer	Minimum value: 1 Maximum value: 65535	
status	Enable/disable the active status of scanning for this protocol.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

Parameter	Description	Type	Size	Default						
inspect-all	Enable/disable the inspection of all ports for the protocol.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
proxy-after-tcp-handshake	Proxy traffic after the TCP 3-way handshake has been established (not before).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
options	One or more options that can be applied to the session.	option	-							
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>oversize</i></td><td>Block oversized file.</td></tr><tr><td><i>splice</i></td><td>Enable splice mode.</td></tr></table>	Option	Description	<i>oversize</i>	Block oversized file.	<i>splice</i>	Enable splice mode.			
Option	Description									
<i>oversize</i>	Block oversized file.									
<i>splice</i>	Enable splice mode.									
oversize-limit	Maximum in-memory file size that can be scanned.	integer	Minimum value: 1 Maximum value: 1606 **	10						
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned.	integer	Minimum value: 1 Maximum value: 1606 **	10						
uncompressed-nest-limit	Maximum nested levels of compression that can be uncompressed and scanned.	integer	Minimum value: 2 Maximum value: 100	12						
scan-bzip2	Enable/disable scanning of BZip2 compressed files.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									

\*\* Values may differ between models.

## config pop3

Parameter	Description	Type	Size	Default
ports	Ports to scan for content.	integer	Minimum value: 1 Maximum value: 65535	
status	Enable/disable the active status of scanning for this protocol.	option	-	enable
	Option	Description		
	enable	Enable setting.		
	disable	Disable setting.		
inspect-all	Enable/disable the inspection of all ports for the protocol.	option	-	disable
	Option	Description		
	enable	Enable setting.		
	disable	Disable setting.		
proxy-after-tcp-handshake	Proxy traffic after the TCP 3-way handshake has been established (not before).	option	-	disable
	Option	Description		
	enable	Enable setting.		
	disable	Disable setting.		
options	One or more options that can be applied to the session.	option	-	
	Option	Description		
	fragmail	Pass fragmented email.		
	oversize	Block oversized email.		
oversize-limit	Maximum in-memory file size that can be scanned.	integer	Minimum value: 1 Maximum value: 1606 **	10

Parameter	Description	Type	Size	Default
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned.	integer	Minimum value: 1 Maximum value: 1606 **	10
uncompressed-nest-limit	Maximum nested levels of compression that can be uncompressed and scanned.	integer	Minimum value: 2 Maximum value: 100	12
scan-bzip2	Enable/disable scanning of BZip2 compressed files.	option	-	enable
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
ssl-offloaded	SSL decryption and encryption performed by an external device.	option	-	no
	<b>Option</b> <b>Description</b>			
	<i>no</i>	SSL decryption and encryption performed by FortiGate when deep-inspection is enabled.		
	<i>yes</i>	SSL decryption and encryption performed by an external device.		

\*\* Values may differ between models.

## config smtp

Parameter	Description	Type	Size	Default
ports	Ports to scan for content.	integer	Minimum value: 1 Maximum value: 65535	
status	Enable/disable the active status of scanning for this protocol.	option	-	enable
	Option	Description		
	enable	Enable setting.		
	disable	Disable setting.		

Parameter	Description	Type	Size	Default
inspect-all	Enable/disable the inspection of all ports for the protocol.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
proxy-after-tcp-handshake	Proxy traffic after the TCP 3-way handshake has been established (not before).	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
options	One or more options that can be applied to the session.	option	-	
	<b>Option</b>	<b>Description</b>		
	<i>fragmail</i>	Pass fragmented email.		
	<i>oversize</i>	Block oversized email.		
	<i>splice</i>	Enable splice mode.		
oversize-limit	Maximum in-memory file size that can be scanned.	integer	Minimum value: 1 Maximum value: 1606 **	10
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned.	integer	Minimum value: 1 Maximum value: 1606 **	10
uncompressed-nest-limit	Maximum nested levels of compression that can be uncompressed and scanned.	integer	Minimum value: 2 Maximum value: 100	12
scan-bzip2	Enable/disable scanning of BZip2 compressed files.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

Parameter	Description	Type	Size	Default
server-busy	Enable/disable SMTP server busy when server not available.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
ssl-offloaded	SSL decryption and encryption performed by an external device.	option	-	no
	<b>Option</b>	<b>Description</b>		
	<i>no</i>	SSL decryption and encryption performed by FortiGate when deep-inspection is enabled.		
	<i>yes</i>	SSL decryption and encryption performed by an external device.		

\*\* Values may differ between models.

## config ssh

Parameter	Description	Type	Size	Default
options	One or more options that can be applied to the session.	option	-	
	<b>Option</b>	<b>Description</b>		
	<i>oversize</i>	Block oversized file.		
	<i>clientcomfort</i>	Prevent client timeout.		
	<i>servercomfort</i>	Prevent server timeout.		
comfort-interval	Period of time between start, or last transmission, and the next client comfort transmission of data.	integer	Minimum value: 1 Maximum value: 900	10
comfort-amount	Amount of data to send in a transmission for client comforting.	integer	Minimum value: 1 Maximum value: 65535	1
oversize-limit	Maximum in-memory file size that can be scanned.	integer	Minimum value: 1 Maximum value: 1606 **	10

Parameter	Description	Type	Size	Default										
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned.	integer	Minimum value: 1 Maximum value: 1606 **	10										
uncompressed-nest-limit	Maximum nested levels of compression that can be uncompressed and scanned.	integer	Minimum value: 2 Maximum value: 100	12										
stream-based-uncompressed-limit	Maximum stream-based uncompressed data size that will be scanned in megabytes. Stream-based uncompression used only under certain conditions.	integer	Minimum value: 0 Maximum value: 4294967295	0										
scan-bzip2	Enable/disable scanning of BZip2 compressed files.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.							
Option	Description													
<i>enable</i>	Enable setting.													
<i>disable</i>	Disable setting.													
tcp-window-type	TCP window type to use for this protocol.	option	-	auto-tuning										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto-tuning</i></td><td>Allow system to auto-tune TCP window size (default).</td></tr><tr><td><i>system</i></td><td>Use system default TCP window size for this protocol.</td></tr><tr><td><i>static</i></td><td>Manually specify TCP window size.</td></tr><tr><td><i>dynamic</i></td><td>Vary TCP window size based on available memory and within limits of tcp-window-minimum and tcp-window-maximum.</td></tr></table>	Option	Description	<i>auto-tuning</i>	Allow system to auto-tune TCP window size (default).	<i>system</i>	Use system default TCP window size for this protocol.	<i>static</i>	Manually specify TCP window size.	<i>dynamic</i>	Vary TCP window size based on available memory and within limits of tcp-window-minimum and tcp-window-maximum.			
Option	Description													
<i>auto-tuning</i>	Allow system to auto-tune TCP window size (default).													
<i>system</i>	Use system default TCP window size for this protocol.													
<i>static</i>	Manually specify TCP window size.													
<i>dynamic</i>	Vary TCP window size based on available memory and within limits of tcp-window-minimum and tcp-window-maximum.													
tcp-window-minimum	Minimum dynamic TCP window size.	integer	Minimum value: 65536 Maximum value: 1048576	131072										
tcp-window-maximum	Maximum dynamic TCP window size.	integer	Minimum value: 1048576 Maximum value: 33554432	8388608										

Parameter	Description	Type	Size	Default
tcp-window-size	Set TCP static window size.	integer	Minimum value: 65536 Maximum value: 33554432	262144
ssl-offloaded	SSL decryption and encryption performed by an external device.	option	-	no
	Option	Description		
	no	SSL decryption and encryption performed by FortiGate when deep-inspection is enabled.		
	yes	SSL decryption and encryption performed by an external device.		

\*\* Values may differ between models.

## config firewall proxy-address

Configure web proxy address.

```
config firewall proxy-address
  Description: Configure web proxy address.
  edit <name>
    set case-sensitivity [disable|enable]
    set category <id1>, <id2>, ...
    set color {integer}
    set comment {var-string}
    set header {string}
    config header-group
      Description: HTTP header group.
      edit <id>
        set header-name {string}
        set header {string}
        set case-sensitivity [disable|enable]
      next
    end
    set header-name {string}
    set host {string}
    set host-regex {string}
    set method {option1}, {option2}, ...
    set path {string}
    set query {string}
    set referrer [enable|disable]
    config tagging
      Description: Config object tagging.
      edit <name>
        set category {string}
        set tags <name1>, <name2>, ...
      next
    end
```



```

        set type [host-regex|url|...]
        set ua {option1}, {option2}, ...
        set uuid {uuid}
    next
end

```

## config firewall proxy-address

Parameter	Description	Type	Size	Default
case-sensitivity	Enable to make the pattern case sensitive.	option	-	disable
	<div><div>Option</div><div>Description</div></div>			
	<div><div>disable</div><div>Case insensitive in pattern.</div></div>			
	<div><div>enable</div><div>Case sensitive in pattern.</div></div>			
category<id>	FortiGuard category ID. FortiGuard category ID.	integer	Minimum value: 0 Maximum value: 4294967295	
color	Integer value to determine the color of the icon in the GUI.	integer	Minimum value: 0 Maximum value: 32	0
comment	Optional comments.	var-string	Maximum length: 255	
header	HTTP header name as a regular expression.	string	Maximum length: 255	
header-name	Name of HTTP header.	string	Maximum length: 79	
host	Address object for the host.	string	Maximum length: 79	
host-regex	Host name as a regular expression.	string	Maximum length: 255	
method	HTTP request methods to be used.	option	-	
	<div><div>Option</div><div>Description</div></div>			
	<div><div>get</div><div>GET method.</div></div>			
	<div><div>post</div><div>POST method.</div></div>			
	<div><div>put</div><div>PUT method.</div></div>			

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>head</i>	HEAD method.		
	<i>connect</i>	CONNECT method.		
	<i>trace</i>	TRACE method.		
	<i>options</i>	OPTIONS method.		
	<i>delete</i>	DELETE method.		
name	Address name.	string	Maximum length: 35	
path	URL path as a regular expression.	string	Maximum length: 255	
query	Match the query part of the URL as a regular expression.	string	Maximum length: 255	
referrer	Enable/disable use of referrer field in the HTTP header to match the address.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
type	Proxy address type.	option	-	url
	<b>Option</b>	<b>Description</b>		
	<i>host-regex</i>	Host regular expression.		
	<i>url</i>	HTTP URL.		
	<i>category</i>	FortiGuard URL category.		
	<i>method</i>	HTTP request method.		
	<i>ua</i>	HTTP request user agent.		
	<i>header</i>	HTTP request header.		
	<i>src-advanced</i>	HTTP advanced source criteria.		
	<i>dst-advanced</i>	HTTP advanced destination criteria.		
ua	Names of browsers to be used as user agent.	option	-	
	<b>Option</b>	<b>Description</b>		
	<i>chrome</i>	Google Chrome.		

Parameter	Description	Type	Size	Default											
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ms</i></td><td>Microsoft Internet Explorer or EDGE.</td></tr><tr><td><i>firefox</i></td><td>Mozilla Firefox.</td></tr><tr><td><i>safari</i></td><td>Apple Safari.</td></tr><tr><td><i>other</i></td><td>Other browsers.</td></tr></table>		Option	Description	<i>ms</i>	Microsoft Internet Explorer or EDGE.	<i>firefox</i>	Mozilla Firefox.	<i>safari</i>	Apple Safari.	<i>other</i>	Other browsers.			
	Option	Description													
	<i>ms</i>	Microsoft Internet Explorer or EDGE.													
	<i>firefox</i>	Mozilla Firefox.													
	<i>safari</i>	Apple Safari.													
	<i>other</i>	Other browsers.													
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000											

### config header-group

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
header-name	HTTP header.	string	Maximum length: 79	
header	HTTP header regular expression.	string	Maximum length: 255	
case-sensitivity	Case sensitivity in pattern.	option	-	disable
	Option	Description		
	disable	Case insensitive in pattern.		
	enable	Case sensitive in pattern.		

### config tagging

Parameter	Description	Type	Size	Default
name	Tagging entry name.	string	Maximum length: 63	
category	Tag category.	string	Maximum length: 63	
tags <name>	Tags. Tag name.	string	Maximum length: 79	

## config firewall proxy-addrgrp

Configure web proxy address group.

```
config firewall proxy-addrgrp
  Description: Configure web proxy address group.
  edit <name>
    set color {integer}
    set comment {var-string}
    set member <name1>, <name2>, ...
    config tagging
      Description: Config object tagging.
      edit <name>
        set category {string}
        set tags <name1>, <name2>, ...
      next
    end
    set type [src|dst]
    set uuid {uuid}
  next
end
```

## config firewall proxy-addrgrp

Parameter	Description	Type	Size	Default						
color	Integer value to determine the color of the icon in the GUI.	integer	Minimum value: 0 Maximum value: 32	0						
comment	Optional comments.	var-string	Maximum length: 255							
member <name>	Members of address group. Address name.	string	Maximum length: 79							
name	Address group name.	string	Maximum length: 63							
type	Source or destination address group type.	option	-	src						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>src</td><td>Source group.</td></tr><tr><td>dst</td><td>Destination group.</td></tr></table>				Option	Description	src	Source group.	dst	Destination group.
Option	Description									
src	Source group.									
dst	Destination group.									
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000						

## config tagging

Parameter	Description	Type	Size	Default
name	Tagging entry name.	string	Maximum length: 63	
category	Tag category.	string	Maximum length: 63	
tags <name>	Tags. Tag name.	string	Maximum length: 79	

## config firewall proxy-policy

Configure proxy policies.

```
config firewall proxy-policy
  Description: Configure proxy policies.
  edit <policyid>
    set access-proxy <name1>, <name2>, ...
    set access-proxy6 <name1>, <name2>, ...
    set action [accept|deny|...]
    set application-list {string}
    set av-profile {string}
    set block-notification [enable|disable]
    set comments {var-string}
    set decrypted-traffic-mirror {string}
    set device-ownership [enable|disable]
    set disclaimer [disable|domain|...]
    set dlp-sensor {string}
    set dstaddr <name1>, <name2>, ...
    set dstaddr-negate [enable|disable]
    set dstaddr6 <name1>, <name2>, ...
    set dstintf <name1>, <name2>, ...
    set emailfilter-profile {string}
    set file-filter-profile {string}
    set groups <name1>, <name2>, ...
    set http-tunnel-auth [enable|disable]
    set icap-profile {string}
    set internet-service [enable|disable]
    set internet-service-custom <name1>, <name2>, ...
    set internet-service-custom-group <name1>, <name2>, ...
    set internet-service-group <name1>, <name2>, ...
    set internet-service-name <name1>, <name2>, ...
    set internet-service-negate [enable|disable]
    set ips-sensor {string}
    set logtraffic [all|utm|...]
    set logtraffic-start [enable|disable]
    set name {string}
    set poolname <name1>, <name2>, ...
    set profile-group {string}
    set profile-protocol-options {string}
    set profile-type [single|group]
```

```

set proxy [explicit-web|transparent-web|...]
set redirect-url {var-string}
set replacemsg-override-group {string}
set schedule {string}
set service <name1>, <name2>, ...
set service-negate [enable|disable]
set session-ttl {integer}
set srcaddr <name1>, <name2>, ...
set srcaddr-negate [enable|disable]
set srcaddr6 <name1>, <name2>, ...
set srcintf <name1>, <name2>, ...
set ssh-filter-profile {string}
set ssh-policy-redirect [enable|disable]
set ssl-ssh-profile {string}
set status [enable|disable]
set transparent [enable|disable]
set users <name1>, <name2>, ...
set utm-status [enable|disable]
set uuid {uuid}
set videofilter-profile {string}
set waf-profile {string}
set webcache [enable|disable]
set webcache-https [disable|enable]
set webfilter-profile {string}
set webproxy-forward-server {string}
set webproxy-profile {string}
set ztna-ems-tag <name1>, <name2>, ...
set ztna-tags-match-logic [or|and]

```

next

end

## config firewall proxy-policy

Parameter	Description	Type	Size	Default								
access-proxy <name>	IPv4 access proxy. Access Proxy name.	string	Maximum length: 79									
access-proxy6 <name>	IPv6 access proxy. Access proxy name.	string	Maximum length: 79									
action	Accept or deny traffic matching the policy parameters.	option	-	deny								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>accept</i></td><td>Action accept.</td></tr><tr><td><i>deny</i></td><td>Action deny.</td></tr><tr><td><i>redirect</i></td><td>Action redirect.</td></tr></table>				Option	Description	<i>accept</i>	Action accept.	<i>deny</i>	Action deny.	<i>redirect</i>	Action redirect.
Option	Description											
<i>accept</i>	Action accept.											
<i>deny</i>	Action deny.											
<i>redirect</i>	Action redirect.											
application-list	Name of an existing Application list.	string	Maximum length: 35									

Parameter	Description	Type	Size	Default										
av-profile	Name of an existing Antivirus profile.	string	Maximum length: 35											
block-notification	Enable/disable block notification.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.							
Option	Description													
<i>enable</i>	Enable setting.													
<i>disable</i>	Disable setting.													
comments	Optional comments.	var-string	Maximum length: 1023											
decrypted-traffic-mirror	Decrypted traffic mirror.	string	Maximum length: 35											
device-ownership	When enabled, the ownership enforcement will be done at policy level.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable device ownership.</td></tr><tr><td><i>disable</i></td><td>Disable device ownership.</td></tr></table>	Option	Description	<i>enable</i>	Enable device ownership.	<i>disable</i>	Disable device ownership.							
Option	Description													
<i>enable</i>	Enable device ownership.													
<i>disable</i>	Disable device ownership.													
disclaimer	Web proxy disclaimer setting: by domain, policy, or user.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable disclaimer.</td></tr><tr><td><i>domain</i></td><td>Display disclaimer for domain</td></tr><tr><td><i>policy</i></td><td>Display disclaimer for policy</td></tr><tr><td><i>user</i></td><td>Display disclaimer for current user</td></tr></table>	Option	Description	<i>disable</i>	Disable disclaimer.	<i>domain</i>	Display disclaimer for domain	<i>policy</i>	Display disclaimer for policy	<i>user</i>	Display disclaimer for current user			
Option	Description													
<i>disable</i>	Disable disclaimer.													
<i>domain</i>	Display disclaimer for domain													
<i>policy</i>	Display disclaimer for policy													
<i>user</i>	Display disclaimer for current user													
dlp-sensor	Name of an existing DLP sensor.	string	Maximum length: 35											
dstaddr <name>	Destination address objects. Address name.	string	Maximum length: 79											
dstaddr-negate	When enabled, destination addresses match against any address EXCEPT the specified destination addresses.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable source address negate.</td></tr></table>	Option	Description	<i>enable</i>	Enable source address negate.									
Option	Description													
<i>enable</i>	Enable source address negate.													

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable destination address negate.</td></tr></table>	Option	Description	<i>disable</i>	Disable destination address negate.					
Option	Description									
<i>disable</i>	Disable destination address negate.									
dstaddr6 <name>	IPv6 destination address objects. Address name.	string	Maximum length: 79							
dstintf <name>	Destination interface names. Interface name.	string	Maximum length: 79							
emailfilter- profile	Name of an existing email filter profile.	string	Maximum length: 35							
file-filter-profile	Name of an existing file-filter profile.	string	Maximum length: 35							
groups <name>	Names of group objects. Group name.	string	Maximum length: 79							
http-tunnel- auth	Enable/disable HTTP tunnel authentication.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
icap-profile	Name of an existing ICAP profile.	string	Maximum length: 35							
internet- service	Enable/disable use of Internet Services for this policy. If enabled, destination address and service are not used.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable use of Internet Services in policy.</td></tr><tr><td><i>disable</i></td><td>Disable use of Internet Services in policy.</td></tr></table>	Option	Description	<i>enable</i>	Enable use of Internet Services in policy.	<i>disable</i>	Disable use of Internet Services in policy.			
Option	Description									
<i>enable</i>	Enable use of Internet Services in policy.									
<i>disable</i>	Disable use of Internet Services in policy.									
internet- service- custom <name>	Custom Internet Service name. Custom Internet Service name.	string	Maximum length: 79							
internet- service- custom-group <name>	Custom Internet Service group name. Custom Internet Service group name.	string	Maximum length: 79							



Parameter	Description	Type	Size	Default								
internet-service-group <name>	Internet Service group name. Internet Service group name.	string	Maximum length: 79									
internet-service-name <name>	Internet Service name. Internet Service name.	string	Maximum length: 79									
internet-service-negate	When enabled, Internet Services match against any internet service EXCEPT the selected Internet Service.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable negated Internet Service match.</td></tr><tr><td>disable</td><td>Disable negated Internet Service match.</td></tr></table>				Option	Description	enable	Enable negated Internet Service match.	disable	Disable negated Internet Service match.		
Option	Description											
enable	Enable negated Internet Service match.											
disable	Disable negated Internet Service match.											
ips-sensor	Name of an existing IPS sensor.	string	Maximum length: 35									
logtraffic	Enable/disable logging traffic through the policy.	option	-	utm								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>all</td><td>Log all sessions.</td></tr><tr><td>utm</td><td>UTM event and matched application traffic log.</td></tr><tr><td>disable</td><td>Disable traffic and application log.</td></tr></table>				Option	Description	all	Log all sessions.	utm	UTM event and matched application traffic log.	disable	Disable traffic and application log.
Option	Description											
all	Log all sessions.											
utm	UTM event and matched application traffic log.											
disable	Disable traffic and application log.											
logtraffic-start	Enable/disable policy log traffic start.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>				Option	Description	enable	Enable setting.	disable	Disable setting.		
Option	Description											
enable	Enable setting.											
disable	Disable setting.											
name	Policy name.	string	Maximum length: 35									
policyid	Policy ID.	integer	Minimum value: 0 Maximum value: 4294967295	0								
poolname <name>	Name of IP pool object. IP pool name.	string	Maximum length: 79									

Parameter	Description	Type	Size	Default																
profile-group	Name of profile group.	string	Maximum length: 35																	
profile-protocol-options	Name of an existing Protocol options profile.	string	Maximum length: 35	default																
profile-type	Determine whether the firewall policy allows security profile groups or single profiles only.	option	-	single																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>single</i></td><td>Do not allow security profile groups.</td></tr><tr><td><i>group</i></td><td>Allow security profile groups.</td></tr></table>	Option	Description	<i>single</i>	Do not allow security profile groups.	<i>group</i>	Allow security profile groups.													
Option	Description																			
<i>single</i>	Do not allow security profile groups.																			
<i>group</i>	Allow security profile groups.																			
proxy	Type of explicit proxy.	option	-																	
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>explicit-web</i></td><td>Explicit Web Proxy</td></tr><tr><td><i>transparent-web</i></td><td>Transparent Web Proxy</td></tr><tr><td><i>ftp</i></td><td>Explicit FTP Proxy</td></tr><tr><td><i>ssh</i></td><td>SSH Proxy</td></tr><tr><td><i>ssh-tunnel</i></td><td>SSH Tunnel</td></tr><tr><td><i>access-proxy</i></td><td>Access Proxy</td></tr><tr><td><i>wanopt</i></td><td>WANopt Tunnel</td></tr></table>	Option	Description	<i>explicit-web</i>	Explicit Web Proxy	<i>transparent-web</i>	Transparent Web Proxy	<i>ftp</i>	Explicit FTP Proxy	<i>ssh</i>	SSH Proxy	<i>ssh-tunnel</i>	SSH Tunnel	<i>access-proxy</i>	Access Proxy	<i>wanopt</i>	WANopt Tunnel			
Option	Description																			
<i>explicit-web</i>	Explicit Web Proxy																			
<i>transparent-web</i>	Transparent Web Proxy																			
<i>ftp</i>	Explicit FTP Proxy																			
<i>ssh</i>	SSH Proxy																			
<i>ssh-tunnel</i>	SSH Tunnel																			
<i>access-proxy</i>	Access Proxy																			
<i>wanopt</i>	WANopt Tunnel																			
redirect-url	Redirect URL for further explicit web proxy processing.	var-string	Maximum length: 1023																	
replacemsg-override-group	Authentication replacement message override group.	string	Maximum length: 35																	
schedule	Name of schedule object.	string	Maximum length: 35																	
service <name>	Name of service objects. Service name.	string	Maximum length: 79																	
service-negate	When enabled, services match against any service EXCEPT the specified destination services.	option	-	disable																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable negated service match.</td></tr><tr><td><i>disable</i></td><td>Disable negated service match.</td></tr></table>	Option	Description	<i>enable</i>	Enable negated service match.	<i>disable</i>	Disable negated service match.													
Option	Description																			
<i>enable</i>	Enable negated service match.																			
<i>disable</i>	Disable negated service match.																			

Parameter	Description	Type	Size	Default						
session-ttl	TTL in seconds for sessions accepted by this policy.	integer	Minimum value: 300 Maximum value: 2764800	0						
srcaddr <name>	Source address objects. Address name.	string	Maximum length: 79							
srcaddr-negate	When enabled, source addresses match against any address EXCEPT the specified source addresses.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable source address negate.</td></tr><tr><td>disable</td><td>Disable destination address negate.</td></tr></table>	Option	Description	enable	Enable source address negate.	disable	Disable destination address negate.			
Option	Description									
enable	Enable source address negate.									
disable	Disable destination address negate.									
srcaddr6 <name>	IPv6 source address objects. Address name.	string	Maximum length: 79							
srcintf <name>	Source interface names. Interface name.	string	Maximum length: 79							
ssh-filter-profile	Name of an existing SSH filter profile.	string	Maximum length: 35							
ssh-policy-redirect	Redirect SSH traffic to matching transparent proxy policy.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable SSH policy redirect.</td></tr><tr><td>disable</td><td>Disable SSH policy redirect.</td></tr></table>	Option	Description	enable	Enable SSH policy redirect.	disable	Disable SSH policy redirect.			
Option	Description									
enable	Enable SSH policy redirect.									
disable	Disable SSH policy redirect.									
ssl-ssh-profile	Name of an existing SSL SSH profile.	string	Maximum length: 35	no-inspection						
status	Enable/disable the active status of the policy.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>	Option	Description	enable	Enable setting.	disable	Disable setting.			
Option	Description									
enable	Enable setting.									
disable	Disable setting.									
transparent	Enable to use the IP address of the client to connect to the server.	option	-	disable						

Parameter	Description	Type	Size	Default
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Enable use of IP address of client to connect to server.		
	<i>disable</i>	Disable use of IP address of client to connect to server.		
users <name>	Names of user objects. Group name.	string	Maximum length: 79	
utm-status	Enable the use of UTM profiles/sensors/lists.	option	-	disable
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000
videofilter-profile	Name of an existing VideoFilter profile.	string	Maximum length: 35	
waf-profile	Name of an existing Web application firewall profile.	string	Maximum length: 35	
webcache *	Enable/disable web caching.	option	-	disable
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
webcache-https *	Enable/disable web caching for HTTPS (Requires deep-inspection enabled in ssl-ssh-profile).	option	-	disable
	<b>Option</b> <b>Description</b>			
	<i>disable</i>	Disable web cache for HTTPS.		
	<i>enable</i>	Enable web cache for HTTPS.		
webfilter-profile	Name of an existing Web filter profile.	string	Maximum length: 35	
webproxy-forward-server	Web proxy forward server name.	string	Maximum length: 63	
webproxy-profile	Name of web proxy profile.	string	Maximum length: 63	

Parameter	Description	Type	Size	Default
ztna-ems-tag <name>	ZTNA EMS Tag names. EMS Tag name.	string	Maximum length: 79	
ztna-tags- match-logic	ZTNA tag matching logic.	option	-	or
	Option	Description		
	<i>or</i>	Match ZTNA tags using a logical OR operator.		
	<i>and</i>	Match ZTNA tags using a logical AND operator.		

\* This parameter may not exist in some models.

## config firewall region

Define region table.

```
config firewall region
    Description: Define region table.
    edit <id>
        set city <id1>, <id2>, ...
        set name {string}
    next
end
```

## config firewall region

Parameter	Description	Type	Size	Default
city <id>	City ID list. City ID.	integer	Minimum value: 0 Maximum value: 65535	
id	Region ID.	integer	Minimum value: 0 Maximum value: 65535	0
name	Region name.	string	Maximum length: 63	

## config firewall schedule group

Schedule group configuration.

```

config firewall schedule group
    Description: Schedule group configuration.
    edit <name>
        set color {integer}
        set fabric-object [enable|disable]
        set member <name1>, <name2>, ...
    next
end

```

## config firewall schedule group

Parameter	Description	Type	Size	Default
color	Color of icon on the GUI.	integer	Minimum value: 0 Maximum value: 32	0
fabric-object	Security Fabric global object setting.	option	-	disable
	Option	Description		
	enable	Object is set as a security fabric-wide global object.		
	disable	Object is local to this security fabric member.		
member <name>	Schedules added to the schedule group. Schedule name.	string	Maximum length: 79	
name	Schedule group name.	string	Maximum length: 31	

## config firewall schedule onetime

Onetime schedule configuration.

```

config firewall schedule onetime
    Description: Onetime schedule configuration.
    edit <name>
        set color {integer}
        set end {user}
        set expiration-days {integer}
        set fabric-object [enable|disable]
        set start {user}
    next
end

```

## config firewall schedule onetime

Parameter	Description	Type	Size	Default						
color	Color of icon on the GUI.	integer	Minimum value: 0 Maximum value: 32	0						
end	Schedule end date and time, format hh:mm yyyy/mm/dd.	user	Not Specified							
expiration-days	Write an event log message this many days before the schedule expires.	integer	Minimum value: 0 Maximum value: 100	3						
fabric-object	Security Fabric global object setting.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Object is set as a security fabric-wide global object.</td></tr><tr><td><i>disable</i></td><td>Object is local to this security fabric member.</td></tr></table>				Option	Description	<i>enable</i>	Object is set as a security fabric-wide global object.	<i>disable</i>	Object is local to this security fabric member.
Option	Description									
<i>enable</i>	Object is set as a security fabric-wide global object.									
<i>disable</i>	Object is local to this security fabric member.									
name	Onetime schedule name.	string	Maximum length: 31							
start	Schedule start date and time, format hh:mm yyyy/mm/dd.	user	Not Specified							

## config firewall schedule recurring

Recurring schedule configuration.

```
config firewall schedule recurring
  Description: Recurring schedule configuration.
  edit <name>
    set color {integer}
    set day {option1}, {option2}, ...
    set end {user}
    set fabric-object [enable|disable]
    set start {user}
  next
end
```

## config firewall schedule recurring

Parameter	Description	Type	Size	Default																		
color	Color of icon on the GUI.	integer	Minimum value: 0 Maximum value: 32	0																		
day	One or more days of the week on which the schedule is valid. Separate the names of the days with a space.	option	-	none																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>sunday</i></td><td>Sunday.</td></tr><tr><td><i>monday</i></td><td>Monday.</td></tr><tr><td><i>tuesday</i></td><td>Tuesday.</td></tr><tr><td><i>wednesday</i></td><td>Wednesday.</td></tr><tr><td><i>thursday</i></td><td>Thursday.</td></tr><tr><td><i>friday</i></td><td>Friday.</td></tr><tr><td><i>saturday</i></td><td>Saturday.</td></tr><tr><td><i>none</i></td><td>None.</td></tr></table>				Option	Description	<i>sunday</i>	Sunday.	<i>monday</i>	Monday.	<i>tuesday</i>	Tuesday.	<i>wednesday</i>	Wednesday.	<i>thursday</i>	Thursday.	<i>friday</i>	Friday.	<i>saturday</i>	Saturday.	<i>none</i>	None.
	Option	Description																				
	<i>sunday</i>	Sunday.																				
	<i>monday</i>	Monday.																				
	<i>tuesday</i>	Tuesday.																				
	<i>wednesday</i>	Wednesday.																				
	<i>thursday</i>	Thursday.																				
	<i>friday</i>	Friday.																				
	<i>saturday</i>	Saturday.																				
<i>none</i>	None.																					
end	Time of day to end the schedule, format hh:mm.	user	Not Specified																			
fabric-object	Security Fabric global object setting.	option	-	disable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Object is set as a security fabric-wide global object.</td></tr><tr><td><i>disable</i></td><td>Object is local to this security fabric member.</td></tr></table>				Option	Description	<i>enable</i>	Object is set as a security fabric-wide global object.	<i>disable</i>	Object is local to this security fabric member.												
	Option	Description																				
	<i>enable</i>	Object is set as a security fabric-wide global object.																				
<i>disable</i>	Object is local to this security fabric member.																					
name	Recurring schedule name.	string	Maximum length: 31																			
start	Time of day to start the schedule, format hh:mm.	user	Not Specified																			

## config firewall security-policy

Configure NGFW IPv4/IPv6 application policies.

```
config firewall security-policy
  Description: Configure NGFW IPv4/IPv6 application policies.
  edit <policyid>
    set action [accept|deny]
    set app-category <id1>, <id2>, ...
```



```

set app-group <name1>, <name2>, ...
set application <id1>, <id2>, ...
set application-list {string}
set av-profile {string}
set cifs-profile {string}
set comments {var-string}
set dlp-sensor {string}
set dnsfilter-profile {string}
set dstaddr <name1>, <name2>, ...
set dstaddr-negate [enable|disable]
set dstaddr6 <name1>, <name2>, ...
set dstintf <name1>, <name2>, ...
set emailfilter-profile {string}
set enforce-default-app-port [enable|disable]
set file-filter-profile {string}
set fsso-groups <name1>, <name2>, ...
set groups <name1>, <name2>, ...
set icap-profile {string}
set internet-service [enable|disable]
set internet-service-custom <name1>, <name2>, ...
set internet-service-custom-group <name1>, <name2>, ...
set internet-service-group <name1>, <name2>, ...
set internet-service-name <name1>, <name2>, ...
set internet-service-negate [enable|disable]
set internet-service-src [enable|disable]
set internet-service-src-custom <name1>, <name2>, ...
set internet-service-src-custom-group <name1>, <name2>, ...
set internet-service-src-group <name1>, <name2>, ...
set internet-service-src-name <name1>, <name2>, ...
set internet-service-src-negate [enable|disable]
set ips-sensor {string}
set learning-mode [enable|disable]
set logtraffic [all|utm|...]
set name {string}
set nat46 [enable|disable]
set nat64 [enable|disable]
set profile-group {string}
set profile-protocol-options {string}
set profile-type [single|group]
set schedule {string}
set sctp-filter-profile {string}
set send-deny-packet [disable|enable]
set service <name1>, <name2>, ...
set service-negate [enable|disable]
set srcaddr <name1>, <name2>, ...
set srcaddr-negate [enable|disable]
set srcaddr6 <name1>, <name2>, ...
set srcintf <name1>, <name2>, ...
set ssh-filter-profile {string}
set ssl-ssh-profile {string}
set status [enable|disable]
set url-category <id1>, <id2>, ...
set users <name1>, <name2>, ...
set uuid {uuid}
set videofilter-profile {string}
set voip-profile {string}

```

```

        set webfilter-profile {string}
    next
end

```

## config firewall security-policy

Parameter	Description	Type	Size	Default
action	Policy action (accept/deny).	option	-	deny
	Option	Description		
	accept	Allows session that match the firewall policy.		
	deny	Blocks sessions that match the firewall policy.		
app-category <id>	Application category ID list. Category IDs.	integer	Minimum value: 0 Maximum value: 4294967295	
app-group <name>	Application group names. Application group names.	string	Maximum length: 79	
application <id>	Application ID list. Application IDs.	integer	Minimum value: 0 Maximum value: 4294967295	
application- list	Name of an existing Application list.	string	Maximum length: 35	
av-profile	Name of an existing Antivirus profile.	string	Maximum length: 35	
cifs-profile	Name of an existing CIFS profile.	string	Maximum length: 35	
comments	Comment.	var-string	Maximum length: 1023	
dlp-sensor	Name of an existing DLP sensor.	string	Maximum length: 35	
dnsfilter- profile	Name of an existing DNS filter profile.	string	Maximum length: 35	
dstaddr <name>	Destination IPv4 address name and address group names. Address name.	string	Maximum length: 79	

Parameter	Description	Type	Size	Default
dstaddr-negate	When enabled dstaddr/dstaddr6 specifies what the destination address must NOT be.	option	-	disable
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Enable destination address negate.		
	<i>disable</i>	Disable destination address negate.		
dstaddr6 <name>	Destination IPv6 address name and address group names. Address name.	string	Maximum length: 79	
dstintf <name>	Outgoing (egress) interface. Interface name.	string	Maximum length: 79	
emailfilter-profile	Name of an existing email filter profile.	string	Maximum length: 35	
enforce-default-app-port	Enable/disable default application port enforcement for allowed applications.	option	-	enable
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
file-filter-profile	Name of an existing file-filter profile.	string	Maximum length: 35	
fsso-groups <name>	Names of FSSO groups. Names of FSSO groups.	string	Maximum length: 511	
groups <name>	Names of user groups that can authenticate with this policy. User group name.	string	Maximum length: 79	
icap-profile	Name of an existing ICAP profile.	string	Maximum length: 35	
internet-service	Enable/disable use of Internet Services for this policy. If enabled, destination address and service are not used.	option	-	disable
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Enable use of Internet Services in policy.		
	<i>disable</i>	Disable use of Internet Services in policy.		

Parameter	Description	Type	Size	Default						
internet-service-custom<name>	Custom Internet Service name. Custom Internet Service name.	string	Maximum length: 79							
internet-service-custom-group<name>	Custom Internet Service group name. Custom Internet Service group name.	string	Maximum length: 79							
internet-service-group<name>	Internet Service group name. Internet Service group name.	string	Maximum length: 79							
internet-service-name<name>	Internet Service name. Internet Service name.	string	Maximum length: 79							
internet-service-negate	When enabled internet-service specifies what the service must NOT be.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable negated Internet Service match.</td></tr><tr><td><i>disable</i></td><td>Disable negated Internet Service match.</td></tr></table>				Option	Description	<i>enable</i>	Enable negated Internet Service match.	<i>disable</i>	Disable negated Internet Service match.
Option	Description									
<i>enable</i>	Enable negated Internet Service match.									
<i>disable</i>	Disable negated Internet Service match.									
internet-service-src	Enable/disable use of Internet Services in source for this policy. If enabled, source address is not used.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable use of Internet Services source in policy.</td></tr><tr><td><i>disable</i></td><td>Disable use of Internet Services source in policy.</td></tr></table>				Option	Description	<i>enable</i>	Enable use of Internet Services source in policy.	<i>disable</i>	Disable use of Internet Services source in policy.
Option	Description									
<i>enable</i>	Enable use of Internet Services source in policy.									
<i>disable</i>	Disable use of Internet Services source in policy.									
internet-service-src-custom<name>	Custom Internet Service source name. Custom Internet Service name.	string	Maximum length: 79							
internet-service-src-custom-group<name>	Custom Internet Service source group name. Custom Internet Service group name.	string	Maximum length: 79							
internet-service-src-group<name>	Internet Service source group name. Internet Service group name.	string	Maximum length: 79							

Parameter	Description	Type	Size	Default								
internet-service-src-name <name>	Internet Service source name. Internet Service name.	string	Maximum length: 79									
internet-service-src-negate	When enabled internet-service-src specifies what the service must NOT be.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable negated Internet Service source match.</td></tr><tr><td>disable</td><td>Disable negated Internet Service source match.</td></tr></table>	Option	Description	enable	Enable negated Internet Service source match.	disable	Disable negated Internet Service source match.					
Option	Description											
enable	Enable negated Internet Service source match.											
disable	Disable negated Internet Service source match.											
ips-sensor	Name of an existing IPS sensor.	string	Maximum length: 35									
learning-mode	Enable to allow everything, but log all of the meaningful data for security information gathering. A learning report will be generated.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable learning mode.</td></tr><tr><td>disable</td><td>Disable learning mode.</td></tr></table>	Option	Description	enable	Enable learning mode.	disable	Disable learning mode.					
Option	Description											
enable	Enable learning mode.											
disable	Disable learning mode.											
logtraffic	Enable or disable logging. Log all sessions or security profile sessions.	option	-	utm								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>all</td><td>Log all sessions accepted or denied by this policy.</td></tr><tr><td>utm</td><td>Log traffic that has a security profile applied to it.</td></tr><tr><td>disable</td><td>Disable all logging for this policy.</td></tr></table>	Option	Description	all	Log all sessions accepted or denied by this policy.	utm	Log traffic that has a security profile applied to it.	disable	Disable all logging for this policy.			
Option	Description											
all	Log all sessions accepted or denied by this policy.											
utm	Log traffic that has a security profile applied to it.											
disable	Disable all logging for this policy.											
name	Policy name.	string	Maximum length: 35									
nat46	Enable/disable NAT46.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable NAT46.</td></tr><tr><td>disable</td><td>Disable NAT46.</td></tr></table>	Option	Description	enable	Enable NAT46.	disable	Disable NAT46.					
Option	Description											
enable	Enable NAT46.											
disable	Disable NAT46.											
nat64	Enable/disable NAT64.	option	-	disable								

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable NAT64.</td></tr><tr><td><i>disable</i></td><td>Disable NAT64.</td></tr></table>				Option	Description	<i>enable</i>	Enable NAT64.	<i>disable</i>	Disable NAT64.
	Option	Description								
	<i>enable</i>	Enable NAT64.								
<i>disable</i>	Disable NAT64.									
policyid	Policy ID.	integer	Minimum value: 0 Maximum value: 4294967294	0						
profile-group	Name of profile group.	string	Maximum length: 35							
profile-protocol-options	Name of an existing Protocol options profile.	string	Maximum length: 35	default						
profile-type	Determine whether the firewall policy allows security profile groups or single profiles only.	option	-	single						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>single</i></td><td>Do not allow security profile groups.</td></tr><tr><td><i>group</i></td><td>Allow security profile groups.</td></tr></table>				Option	Description	<i>single</i>	Do not allow security profile groups.	<i>group</i>	Allow security profile groups.
	Option	Description								
	<i>single</i>	Do not allow security profile groups.								
<i>group</i>	Allow security profile groups.									
schedule	Schedule name.	string	Maximum length: 35							
sctp-filter-profile	Name of an existing SCTP filter profile.	string	Maximum length: 35							
send-deny-packet	Enable to send a reply when a session is denied or blocked by a firewall policy.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable deny-packet sending.</td></tr><tr><td><i>enable</i></td><td>Enable deny-packet sending.</td></tr></table>				Option	Description	<i>disable</i>	Disable deny-packet sending.	<i>enable</i>	Enable deny-packet sending.
	Option	Description								
	<i>disable</i>	Disable deny-packet sending.								
<i>enable</i>	Enable deny-packet sending.									
service <name>	Service and service group names. Service name.	string	Maximum length: 79							
service-negate	When enabled service specifies what the service must NOT be.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable negated service match.</td></tr></table>				Option	Description	<i>enable</i>	Enable negated service match.		
	Option	Description								
<i>enable</i>	Enable negated service match.									

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable negated service match.</td></tr></table>				Option	Description	<i>disable</i>	Disable negated service match.		
	Option	Description								
	<i>disable</i>	Disable negated service match.								
srcaddr <name>	Source IPv4 address name and address group names. Address name.	string	Maximum length: 79							
srcaddr-negate	When enabled srcaddr/srcaddr6 specifies what the source address must NOT be.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable source address negate.</td></tr><tr><td><i>disable</i></td><td>Disable source address negate.</td></tr></table>				Option	Description	<i>enable</i>	Enable source address negate.	<i>disable</i>	Disable source address negate.
	Option	Description								
	<i>enable</i>	Enable source address negate.								
<i>disable</i>	Disable source address negate.									
srcaddr6 <name>	Source IPv6 address name and address group names. Address name.	string	Maximum length: 79							
srcintf <name>	Incoming (ingress) interface. Interface name.	string	Maximum length: 79							
ssh-filter-profile	Name of an existing SSH filter profile.	string	Maximum length: 35							
ssl-ssh-profile	Name of an existing SSL SSH profile.	string	Maximum length: 35	no-inspection						
status	Enable or disable this policy.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>				Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.
	Option	Description								
	<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.									
url-category <id>	URL category ID list. URL category ID.	integer	Minimum value: 0 Maximum value: 4294967295							
users <name>	Names of individual users that can authenticate with this policy. User name.	string	Maximum length: 79							
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000						

Parameter	Description	Type	Size	Default
videofilter-profile	Name of an existing VideoFilter profile.	string	Maximum length: 35	
voip-profile	Name of an existing VoIP profile.	string	Maximum length: 35	
webfilter-profile	Name of an existing Web filter profile.	string	Maximum length: 35	

## config firewall service category

Configure service categories.

```
config firewall service category
    Description: Configure service categories.
    edit <name>
        set comment {var-string}
        set fabric-object [enable|disable]
    next
end
```

## config firewall service category

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 255	
fabric-object	Security Fabric global object setting.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Object is set as a security fabric-wide global object.		
	<i>disable</i>	Object is local to this security fabric member.		
name	Service category name.	string	Maximum length: 63	

## config firewall service custom

Configure custom services.

```
config firewall service custom
    Description: Configure custom services.
    edit <name>
        set app-category <id1>, <id2>, ...
        set app-service-type [disable|app-id|...]
        set application <id1>, <id2>, ...
        set category {string}
```



```

set check-reset-range [disable|strict|...]
set color {integer}
set comment {var-string}
set fabric-object [enable|disable]
set fqdn {string}
set helper [auto|disable|...]
set icmpcode {integer}
set icmptype {integer}
set iprange {user}
set protocol [TCP/UDP/SCTP/ICMP|...]
set protocol-number {integer}
set proxy [enable|disable]
set sctp-portrange {user}
set session-ttl {user}
set tcp-halfclose-timer {integer}
set tcp-halfopen-timer {integer}
set tcp-portrange {user}
set tcp-rst-timer {integer}
set tcp-timewait-timer {integer}
set udp-idle-timer {integer}
set udp-portrange {user}
set visibility [enable|disable]
next
end

```

## config firewall service custom

Parameter	Description	Type	Size	Default
app-category <id>	Application category ID. Application category id.	integer	Minimum value: 0 Maximum value: 4294967295	
app-service- type	Application service type.	option	-	disable
	OptionDescription			
	disable	Disable application type.		
	app-id	Application ID.		
	app-category	Applicatin category.		
application <id>	Application ID. Application id.	integer	Minimum value: 0 Maximum value: 4294967295	
category	Service category.	string	Maximum length: 63	

Parameter	Description	Type	Size	Default
check-reset-range	Configure the type of ICMP error message verification.	option	-	default
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable RST range check.		
	<i>strict</i>	Check RST range strictly.		
	<i>default</i>	Using system default setting.		
color	Color of icon on the GUI.	integer	Minimum value: 0 Maximum value: 32	0
comment	Comment.	var-string	Maximum length: 255	
fabric-object	Security Fabric global object setting.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Object is set as a security fabric-wide global object.		
	<i>disable</i>	Object is local to this security fabric member.		
fqdn	Fully qualified domain name.	string	Maximum length: 255	
helper	Helper name.	option	-	auto
	<b>Option</b>	<b>Description</b>		
	<i>auto</i>	Automatically select helper based on protocol and port.		
	<i>disable</i>	Disable helper.		
	<i>ftp</i>	FTP.		
	<i>tftp</i>	TFTP.		
	<i>ras</i>	RAS.		
	<i>h323</i>	H323.		
	<i>tns</i>	TNS.		
	<i>mms</i>	MMS.		
	<i>sip</i>	SIP.		
	<i>pptp</i>	PPTP.		
	<i>rtsp</i>	RTSP.		

Parameter	Description	Type	Size	Default																							
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>dns-udp</i></td><td>DNS UDP.</td></tr><tr><td><i>dns-tcp</i></td><td>DNS TCP.</td></tr><tr><td><i>pmap</i></td><td>PMap.</td></tr><tr><td><i>rsh</i></td><td>RSH.</td></tr><tr><td><i>dcerpc</i></td><td>DCERPC.</td></tr><tr><td><i>mgcp</i></td><td>MGCP.</td></tr></table>		Option	Description	<i>dns-udp</i>	DNS UDP.	<i>dns-tcp</i>	DNS TCP.	<i>pmap</i>	PMap.	<i>rsh</i>	RSH.	<i>dcerpc</i>	DCERPC.	<i>mgcp</i>	MGCP.											
	Option	Description																									
	<i>dns-udp</i>	DNS UDP.																									
	<i>dns-tcp</i>	DNS TCP.																									
	<i>pmap</i>	PMap.																									
	<i>rsh</i>	RSH.																									
	<i>dcerpc</i>	DCERPC.																									
<i>mgcp</i>	MGCP.																										
icmpcode	ICMP code.	integer	Minimum value: 0 Maximum value: 255																								
icmptype	ICMP type.	integer	Minimum value: 0 Maximum value: 4294967295																								
iprange	Start and end of the IP range associated with service.	user	Not Specified																								
name	Custom service name.	string	Maximum length: 79																								
protocol	Protocol type based on IANA numbers.	option	-	TCP/UDP/SCTP																							
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>TCP/UDP/SCTP</i></td><td>TCP, UDP and SCTP.</td></tr><tr><td><i>ICMP</i></td><td>ICMP.</td></tr><tr><td><i>ICMP6</i></td><td>ICMP6.</td></tr><tr><td><i>IP</i></td><td>IP.</td></tr><tr><td><i>HTTP</i></td><td>HTTP - for web proxy.</td></tr><tr><td><i>FTP</i></td><td>FTP - for web proxy.</td></tr><tr><td><i>CONNECT</i></td><td>Connect - for web proxy.</td></tr><tr><td><i>SOCKS-TCP</i></td><td>Socks TCP - for web proxy.</td></tr><tr><td><i>SOCKS-UDP</i></td><td>Socks UDP - for web proxy.</td></tr><tr><td><i>ALL</i></td><td>All - for web proxy.</td></tr></table>		Option	Description	<i>TCP/UDP/SCTP</i>	TCP, UDP and SCTP.	<i>ICMP</i>	ICMP.	<i>ICMP6</i>	ICMP6.	<i>IP</i>	IP.	<i>HTTP</i>	HTTP - for web proxy.	<i>FTP</i>	FTP - for web proxy.	<i>CONNECT</i>	Connect - for web proxy.	<i>SOCKS-TCP</i>	Socks TCP - for web proxy.	<i>SOCKS-UDP</i>	Socks UDP - for web proxy.	<i>ALL</i>	All - for web proxy.			
	Option	Description																									
	<i>TCP/UDP/SCTP</i>	TCP, UDP and SCTP.																									
	<i>ICMP</i>	ICMP.																									
	<i>ICMP6</i>	ICMP6.																									
	<i>IP</i>	IP.																									
	<i>HTTP</i>	HTTP - for web proxy.																									
	<i>FTP</i>	FTP - for web proxy.																									
	<i>CONNECT</i>	Connect - for web proxy.																									
	<i>SOCKS-TCP</i>	Socks TCP - for web proxy.																									
	<i>SOCKS-UDP</i>	Socks UDP - for web proxy.																									
<i>ALL</i>	All - for web proxy.																										

Parameter	Description	Type	Size	Default
protocol-number	IP protocol number.	integer	Minimum value: 0 Maximum value: 254	0
proxy	Enable/disable web proxy service.	option	-	disable
	Option	Description		
	enable	Enable setting.		
	disable	Disable setting.		
sctp-portrange	Multiple SCTP port ranges.	user	Not Specified	
session-ttl	Session TTL.	user	Not Specified	
tcp-halfclose-timer	Wait time to close a TCP session waiting for an unanswered FIN packet.	integer	Minimum value: 0 Maximum value: 86400	0
tcp-halfopen-timer	Wait time to close a TCP session waiting for an unanswered open session packet.	integer	Minimum value: 0 Maximum value: 86400	0
tcp-portrange	Multiple TCP port ranges.	user	Not Specified	
tcp-rst-timer	Set the length of the TCP CLOSE state in seconds.	integer	Minimum value: 5 Maximum value: 300	0
tcp-timewait-timer	Set the length of the TCP TIME-WAIT state in seconds.	integer	Minimum value: 0 Maximum value: 300	0
udp-idle-timer	UDP half close timeout.	integer	Minimum value: 0 Maximum value: 86400	0
udp-portrange	Multiple UDP port ranges.	user	Not Specified	
visibility	Enable/disable the visibility of the service on the GUI.	option	-	enable

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Show in service selection.		
	<i>disable</i>	Hide from service selection.		

## config firewall service group

Configure service groups.

```
config firewall service group
    Description: Configure service groups.
    edit <name>
        set color {integer}
        set comment {var-string}
        set fabric-object [enable|disable]
        set member <name1>, <name2>, ...
        set proxy [enable|disable]
    next
end
```

## config firewall service group

Parameter	Description	Type	Size	Default
color	Color of icon on the GUI.	integer	Minimum value: 0 Maximum value: 32	0
comment	Comment.	var-string	Maximum length: 255	
fabric-object	Security Fabric global object setting.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Object is set as a security fabric-wide global object.		
	<i>disable</i>	Object is local to this security fabric member.		
member <name>	Service objects contained within the group. Address name.	string	Maximum length: 79	
name	Address group name.	string	Maximum length: 79	
proxy	Enable/disable web proxy service group.	option	-	disable

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

## config firewall shaper per-ip-shaper

Configure per-IP traffic shaper.

```
config firewall shaper per-ip-shaper
  Description: Configure per-IP traffic shaper.
  edit <name>
    set bandwidth-unit [kbps|mbps|...]
    set diffserv-forward [enable|disable]
    set diffserv-reverse [enable|disable]
    set diffservcode-forward {user}
    set diffservcode-rev {user}
    set max-bandwidth {integer}
    set max-concurrent-session {integer}
    set max-concurrent-tcp-session {integer}
    set max-concurrent-udp-session {integer}
  next
end
```

## config firewall shaper per-ip-shaper

Parameter	Description	Type	Size	Default
bandwidth-unit	Unit of measurement for maximum bandwidth for this shaper (Kbps, Mbps or Gbps).	option	-	kbps
	<b>Option</b>	<b>Description</b>		
	<i>kbps</i>	Kilobits per second.		
	<i>mbps</i>	Megabits per second.		
	<i>gbps</i>	Gigabits per second.		
diffserv-forward	Enable/disable changing the Forward (original) DiffServ setting applied to traffic accepted by this shaper.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting forward (original) traffic DiffServ.		
	<i>disable</i>	Disable setting forward (original) traffic DiffServ.		

Parameter	Description	Type	Size	Default						
diffserv-reverse	Enable/disable changing the Reverse (reply) DiffServ setting applied to traffic accepted by this shaper.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting reverse (reply) traffic DiffServ.</td></tr><tr><td><i>disable</i></td><td>Disable setting reverse (reply) traffic DiffServ.</td></tr></table>				Option	Description	<i>enable</i>	Enable setting reverse (reply) traffic DiffServ.	<i>disable</i>	Disable setting reverse (reply) traffic DiffServ.
	Option	Description								
	<i>enable</i>	Enable setting reverse (reply) traffic DiffServ.								
<i>disable</i>	Disable setting reverse (reply) traffic DiffServ.									
diffservcode-forward	Forward (original) DiffServ setting to be applied to traffic accepted by this shaper.	user	Not Specified							
diffservcode-rev	Reverse (reply) DiffServ setting to be applied to traffic accepted by this shaper.	user	Not Specified							
max-bandwidth	Upper bandwidth limit enforced by this shaper. 0 means no limit. Units depend on the bandwidth-unit setting.	integer	Minimum value: 0 Maximum value: 80000000 **	0						
max-concurrent-session	Maximum number of concurrent sessions allowed by this shaper. 0 means no limit.	integer	Minimum value: 0 Maximum value: 2097000	0						
max-concurrent-tcp-session	Maximum number of concurrent TCP sessions allowed by this shaper. 0 means no limit.	integer	Minimum value: 0 Maximum value: 2097000	0						
max-concurrent-udp-session	Maximum number of concurrent UDP sessions allowed by this shaper. 0 means no limit.	integer	Minimum value: 0 Maximum value: 2097000	0						
name	Traffic shaper name.	string	Maximum length: 35							

\*\* Values may differ between models.

## config firewall shaper traffic-shaper

Configure shared traffic shaper.

```
config firewall shaper traffic-shaper
    Description: Configure shared traffic shaper.
    edit <name>
        set bandwidth-unit [kbps|mbps|...]
```

```

set diffserv [enable|disable]
set diffservcode {user}
set dscp-marking-method [multi-stage|static]
set exceed-bandwidth {integer}
set exceed-class-id {integer}
set exceed-dscp {user}
set guaranteed-bandwidth {integer}
set maximum-bandwidth {integer}
set maximum-dscp {user}
set overhead {integer}
set per-policy [disable|enable]
set priority [low|medium|...]
next
end

```

## config firewall shaper traffic-shaper

Parameter	Description	Type	Size	Default								
bandwidth-unit	Unit of measurement for guaranteed and maximum bandwidth for this shaper (Kbps, Mbps or Gbps).	option	-	kbps								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>kbps</i></td><td>Kilobits per second.</td></tr><tr><td><i>mbps</i></td><td>Megabits per second.</td></tr><tr><td><i>gbps</i></td><td>Gigabits per second.</td></tr></table>	Option	Description	<i>kbps</i>	Kilobits per second.	<i>mbps</i>	Megabits per second.	<i>gbps</i>	Gigabits per second.			
Option	Description											
<i>kbps</i>	Kilobits per second.											
<i>mbps</i>	Megabits per second.											
<i>gbps</i>	Gigabits per second.											
diffserv	Enable/disable changing the DiffServ setting applied to traffic accepted by this shaper.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting traffic DiffServ.</td></tr><tr><td><i>disable</i></td><td>Disable setting traffic DiffServ.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting traffic DiffServ.	<i>disable</i>	Disable setting traffic DiffServ.					
Option	Description											
<i>enable</i>	Enable setting traffic DiffServ.											
<i>disable</i>	Disable setting traffic DiffServ.											
diffservcode	DiffServ setting to be applied to traffic accepted by this shaper.	user	Not Specified									
dscp-marking-method	Select DSCP marking method.	option	-	static								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>multi-stage</i></td><td>Multistage marking.</td></tr><tr><td><i>static</i></td><td>Static marking.</td></tr></table>	Option	Description	<i>multi-stage</i>	Multistage marking.	<i>static</i>	Static marking.					
Option	Description											
<i>multi-stage</i>	Multistage marking.											
<i>static</i>	Static marking.											



Parameter	Description	Type	Size	Default						
exceed-bandwidth	Exceed bandwidth used for DSCP multi-stage marking. Units depend on the bandwidth-unit setting.	integer	Minimum value: 0 Maximum value: 80000000 **	0						
exceed-class-id	Class ID for traffic in guaranteed-bandwidth and maximum-bandwidth.	integer	Minimum value: 0 Maximum value: 4294967295	0						
exceed-dscp	DSCP mark for traffic in guaranteed-bandwidth and exceed-bandwidth.	user	Not Specified							
guaranteed-bandwidth	Amount of bandwidth guaranteed for this shaper. Units depend on the bandwidth-unit setting.	integer	Minimum value: 0 Maximum value: 80000000 **	0						
maximum-bandwidth	Upper bandwidth limit enforced by this shaper. 0 means no limit. Units depend on the bandwidth-unit setting.	integer	Minimum value: 0 Maximum value: 80000000 **	0						
maximum-dscp	DSCP mark for traffic in exceed-bandwidth and maximum-bandwidth.	user	Not Specified							
name	Traffic shaper name.	string	Maximum length: 35							
overhead	Per-packet size overhead used in rate computations.	integer	Minimum value: 0 Maximum value: 100	0						
per-policy	Enable/disable applying a separate shaper for each policy. For example, if enabled the guaranteed bandwidth is applied separately for each policy.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>All referring policies share one traffic shaper.</td></tr><tr><td>enable</td><td>Each referring policy has its own traffic shaper.</td></tr></table>				Option	Description	disable	All referring policies share one traffic shaper.	enable	Each referring policy has its own traffic shaper.
	Option	Description								
	disable	All referring policies share one traffic shaper.								
enable	Each referring policy has its own traffic shaper.									
priority	Higher priority traffic is more likely to be forwarded without delays and without compromising the guaranteed bandwidth.	option	-	high						

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>low</i>	Low priority.		
	<i>medium</i>	Medium priority.		
	<i>high</i>	High priority.		

\*\* Values may differ between models.

## config firewall shaping-policy

Configure shaping policies.

```
config firewall shaping-policy
  Description: Configure shaping policies.
  edit <id>
    set app-category <id1>, <id2>, ...
    set app-group <name1>, <name2>, ...
    set application <id1>, <id2>, ...
    set class-id {integer}
    set comment {var-string}
    set diffserv-forward [enable|disable]
    set diffserv-reverse [enable|disable]
    set diffservcode-forward {user}
    set diffservcode-rev {user}
    set dstaddr <name1>, <name2>, ...
    set dstaddr6 <name1>, <name2>, ...
    set dstintf <name1>, <name2>, ...
    set groups <name1>, <name2>, ...
    set internet-service [enable|disable]
    set internet-service-custom <name1>, <name2>, ...
    set internet-service-custom-group <name1>, <name2>, ...
    set internet-service-group <name1>, <name2>, ...
    set internet-service-name <name1>, <name2>, ...
    set internet-service-src [enable|disable]
    set internet-service-src-custom <name1>, <name2>, ...
    set internet-service-src-custom-group <name1>, <name2>, ...
    set internet-service-src-group <name1>, <name2>, ...
    set internet-service-src-name <name1>, <name2>, ...
    set ip-version [4|6]
    set name {string}
    set per-ip-shaper {string}
    set schedule {string}
    set service <name1>, <name2>, ...
    set srcaddr <name1>, <name2>, ...
    set srcaddr6 <name1>, <name2>, ...
    set srcintf <name1>, <name2>, ...
    set status [enable|disable]
    set tos {user}
    set tos-mask {user}
    set tos-negate [enable|disable]
    set traffic-shaper {string}
```

```

    set traffic-shaper-reverse {string}
    set url-category <id1>, <id2>, ...
    set users <name1>, <name2>, ...
next
end

```

## config firewall shaping-policy

Parameter	Description	Type	Size	Default
app-category <id>	IDs of one or more application categories that this shaper applies application control traffic shaping to. Category IDs.	integer	Minimum value: 0 Maximum value: 4294967295	
app-group <name>	One or more application group names. Application group name.	string	Maximum length: 79	
application <id>	IDs of one or more applications that this shaper applies application control traffic shaping to. Application IDs.	integer	Minimum value: 0 Maximum value: 4294967295	
class-id	Traffic class ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
comment	Comments.	var-string	Maximum length: 255	
diffserv-forward	Enable to change packet's DiffServ values to the specified diffservcode-forward value.	option	-	disable
	<b>Option</b>		<b>Description</b>	
	<i>enable</i>		Enable setting forward (original) traffic DiffServ.	
	<i>disable</i>		Disable setting forward (original) traffic DiffServ.	
diffserv-reverse	Enable to change packet's reverse (reply) DiffServ values to the specified diffservcode-rev value.	option	-	disable
	<b>Option</b>		<b>Description</b>	
	<i>enable</i>		Enable setting reverse (reply) traffic DiffServ.	
	<i>disable</i>		Disable setting reverse (reply) traffic DiffServ.	

Parameter	Description	Type	Size	Default						
diffservcode-forward	Change packet's DiffServ to this value.	user	Not Specified							
diffservcode-rev	Change packet's reverse (reply) DiffServ to this value.	user	Not Specified							
dstaddr <name>	IPv4 destination address and address group names. Address name.	string	Maximum length: 79							
dstaddr6 <name>	IPv6 destination address and address group names. Address name.	string	Maximum length: 79							
dstintf <name>	One or more outgoing (egress) interfaces. Interface name.	string	Maximum length: 79							
groups <name>	Apply this traffic shaping policy to user groups that have authenticated with the FortiGate. Group name.	string	Maximum length: 79							
id	Shaping policy ID.	integer	Minimum value: 0 Maximum value: 4294967295	0						
internet-service	Enable/disable use of Internet Services for this policy. If enabled, destination address and service are not used.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable use of Internet Service in shaping-policy.</td></tr><tr><td>disable</td><td>Disable use of Internet Service in shaping-policy.</td></tr></table>				Option	Description	enable	Enable use of Internet Service in shaping-policy.	disable	Disable use of Internet Service in shaping-policy.
Option	Description									
enable	Enable use of Internet Service in shaping-policy.									
disable	Disable use of Internet Service in shaping-policy.									
internet-service-custom <name>	Custom Internet Service name. Custom Internet Service name.	string	Maximum length: 79							
internet-service-custom-group <name>	Custom Internet Service group name. Custom Internet Service group name.	string	Maximum length: 79							
internet-service-group <name>	Internet Service group name. Internet Service group name.	string	Maximum length: 79							
internet-service-name <name>	Internet Service ID. Internet Service name.	string	Maximum length: 79							

Parameter	Description	Type	Size	Default						
internet-service-src	Enable/disable use of Internet Services in source for this policy. If enabled, source address is not used.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable use of Internet Service source in shaping-policy.</td></tr><tr><td>disable</td><td>Disable use of Internet Service source in shaping-policy.</td></tr></table>	Option	Description	enable	Enable use of Internet Service source in shaping-policy.	disable	Disable use of Internet Service source in shaping-policy.			
Option	Description									
enable	Enable use of Internet Service source in shaping-policy.									
disable	Disable use of Internet Service source in shaping-policy.									
internet-service-src-custom <name>	Custom Internet Service source name. Custom Internet Service name.	string	Maximum length: 79							
internet-service-src-custom-group <name>	Custom Internet Service source group name. Custom Internet Service group name.	string	Maximum length: 79							
internet-service-src-group <name>	Internet Service source group name. Internet Service group name.	string	Maximum length: 79							
internet-service-src-name <name>	Internet Service source name. Internet Service name.	string	Maximum length: 79							
ip-version	Apply this traffic shaping policy to IPv4 or IPv6 traffic.	option	-	4						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>4</td><td>Use IPv4 addressing for Configuration Method.</td></tr><tr><td>6</td><td>Use IPv6 addressing for Configuration Method.</td></tr></table>	Option	Description	4	Use IPv4 addressing for Configuration Method.	6	Use IPv6 addressing for Configuration Method.			
Option	Description									
4	Use IPv4 addressing for Configuration Method.									
6	Use IPv6 addressing for Configuration Method.									
name	Shaping policy name.	string	Maximum length: 35							
per-ip-shaper	Per-IP traffic shaper to apply with this policy.	string	Maximum length: 35							
schedule	Schedule name.	string	Maximum length: 35							
service <name>	Service and service group names. Service name.	string	Maximum length: 79							
srcaddr <name>	IPv4 source address and address group names. Address name.	string	Maximum length: 79							
srcaddr6 <name>	IPv6 source address and address group names. Address name.	string	Maximum length: 79							

Parameter	Description	Type	Size	Default
srcintf <name>	One or more incoming (ingress) interfaces. Interface name.	string	Maximum length: 79	
status	Enable/disable this traffic shaping policy.	option	-	enable
	Option	Description		
	enable	Enable traffic shaping policy.		
	disable	Disable traffic shaping policy.		
tos	ToS (Type of Service) value used for comparison.	user	Not Specified	
tos-mask	Non-zero bit positions are used for comparison while zero bit positions are ignored.	user	Not Specified	
tos-negate	Enable negated TOS match.	option	-	disable
	Option	Description		
	enable	Enable TOS match negate.		
	disable	Disable TOS match negate.		
traffic-shaper	Traffic shaper to apply to traffic forwarded by the firewall policy.	string	Maximum length: 35	
traffic-shaper-reverse	Traffic shaper to apply to response traffic received by the firewall policy.	string	Maximum length: 35	
url-category <id>	IDs of one or more FortiGuard Web Filtering categories that this shaper applies traffic shaping to. URL category ID.	integer	Minimum value: 0 Maximum value: 4294967295	
users <name>	Apply this traffic shaping policy to individual users that have authenticated with the FortiGate. User name.	string	Maximum length: 79	

## config firewall shaping-profile

Configure shaping profiles.

```
config firewall shaping-profile
  Description: Configure shaping profiles.
  edit <profile-name>
    set comment {var-string}
    set default-class-id {integer}
    config shaping-entries
      Description: Define shaping entries of this shaping profile.
      edit <id>
        set class-id {integer}
```

```

        set priority [top|critical|...]
        set guaranteed-bandwidth-percentage {integer}
        set maximum-bandwidth-percentage {integer}
        set limit {integer}
        set burst-in-msec {integer}
        set cburst-in-msec {integer}
        set red-probability {integer}
        set min {integer}
        set max {integer}
    next
end
    set type [policing|queuing]
next
end

```

## config firewall shaping-profile

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 1023	
default-class-id	Default class ID to handle unclassified packets (including all local traffic).	integer	Minimum value: 0 Maximum value: 4294967295	0
profile-name	Shaping profile name.	string	Maximum length: 35	
type	Select shaping profile type: policing / queuing.	option	-	policing
	<b>Option</b>	<b>Description</b>		
	<i>policing</i>	Enable policing mode.		
	<i>queuing</i>	Enable queuing mode.		

## config shaping-entries

Parameter	Description	Type	Size	Default
id	ID number.	integer	Minimum value: 0 Maximum value: 4294967295	0

Parameter	Description	Type	Size	Default
class-id	Class ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
priority	Priority.	option	-	high
	Option	Description		
	top	Top priority.		
	critical	Critical priority.		
	high	High priority.		
	medium	Medium priority.		
	low	Low priority.		
	guaranteed-bandwidth-percentage	Guaranteed bandwidth in percentage.	integer	Minimum value: 0 Maximum value: 100
maximum-bandwidth-percentage	Maximum bandwidth in percentage.	integer	Minimum value: 1 Maximum value: 100	1
limit	Hard limit on the real queue size in packets.	integer	Minimum value: 5 Maximum value: 10000	1000
burst-in-msec	Number of bytes that can be burst at maximum-bandwidth speed. Formula: burst = maximum-bandwidth*burst-in-msec.	integer	Minimum value: 0 Maximum value: 2000	0
cburst-in-msec	Number of bytes that can be burst as fast as the interface can transmit. Formula: cburst = maximum-bandwidth*cburst-in-msec.	integer	Minimum value: 0 Maximum value: 2000	0
red-probability	Maximum probability (in percentage) for RED marking.	integer	Minimum value: 0 Maximum value: 20	0



Parameter	Description	Type	Size	Default
min	Average queue size in packets at which RED drop becomes a possibility.	integer	Minimum value: 3 Maximum value: 3000	83
max	Average queue size in packets at which RED drop probability is maximal.	integer	Minimum value: 3 Maximum value: 3000	250

## config firewall sniffer

Configure sniffer.

```

config firewall sniffer
    Description: Configure sniffer.
    edit <id>
        config anomaly
            Description: Configuration method to edit Denial of Service (DoS) anomaly
settings.
            edit <name>
                set status [disable|enable]
                set log [enable|disable]
                set action [pass|block]
                set quarantine [none|attacker]
                set quarantine-expiry {user}
                set quarantine-log [disable|enable]
                set threshold {integer}
                set threshold(default) {integer}
            next
        end
        set application-list {string}
        set application-list-status [enable|disable]
        set av-profile {string}
        set av-profile-status [enable|disable]
        set dlp-sensor {string}
        set dlp-sensor-status [enable|disable]
        set dsri [enable|disable]
        set emailfilter-profile {string}
        set emailfilter-profile-status [enable|disable]
        set file-filter-profile {string}
        set file-filter-profile-status [enable|disable]
        set host {string}
        set interface {string}
        set ip-threatfeed <name1>, <name2>, ...
        set ip-threatfeed-status [enable|disable]
        set ips-dos-status [enable|disable]
        set ips-sensor {string}
        set ips-sensor-status [enable|disable]
        set ipv6 [enable|disable]
        set logtraffic [all|utm|...]
        set max-packet-count {integer}

```

```

        set non-ip [enable|disable]
        set port {string}
        set protocol {string}
        set status [enable|disable]
        set vlan {string}
        set webfilter-profile {string}
        set webfilter-profile-status [enable|disable]
    next
end

```

## config firewall sniffer

Parameter	Description	Type	Size	Default						
application-list	Name of an existing application list.	string	Maximum length: 35							
application-list-status	Enable/disable application control profile.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
av-profile	Name of an existing antivirus profile.	string	Maximum length: 35							
av-profile-status	Enable/disable antivirus profile.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
dlp-sensor	Name of an existing DLP sensor.	string	Maximum length: 35							
dlp-sensor-status	Enable/disable DLP sensor.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
dsri	Enable/disable DSRI.	option	-	disable						

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable DSRI.		
	<i>disable</i>	Disable DSRI.		
emailfilter-profile	Name of an existing email filter profile.	string	Maximum length: 35	
emailfilter-profile-status	Enable/disable emailfilter.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
file-filter-profile	Name of an existing file-filter profile.	string	Maximum length: 35	
file-filter-profile-status	Enable/disable file filter.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
host	Hosts to filter for in sniffer traffic.	string	Maximum length: 63	
id	Sniffer ID.	integer	Minimum value: 0 Maximum value: 9999	0
interface	Interface name that traffic sniffing will take place on.	string	Maximum length: 35	
ip-threatfeed <name>	Name of an existing IP threat feed. Threat feed name.	string	Maximum length: 79	
ip-threatfeed-status	Enable/disable IP threat feed.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

Parameter	Description	Type	Size	Default								
ips-dos-status	Enable/disable IPS DoS anomaly detection.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
ips-sensor	Name of an existing IPS sensor.	string	Maximum length: 35									
ips-sensor-status	Enable/disable IPS sensor.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
ipv6	Enable/disable sniffing IPv6 packets.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable sniffer for IPv6 packets.</td></tr><tr><td><i>disable</i></td><td>Disable sniffer for IPv6 packets.</td></tr></table>	Option	Description	<i>enable</i>	Enable sniffer for IPv6 packets.	<i>disable</i>	Disable sniffer for IPv6 packets.					
Option	Description											
<i>enable</i>	Enable sniffer for IPv6 packets.											
<i>disable</i>	Disable sniffer for IPv6 packets.											
logtraffic	Either log all sessions, only sessions that have a security profile applied, or disable all logging for this policy.	option	-	utm								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>all</i></td><td>Log all sessions accepted or denied by this policy.</td></tr><tr><td><i>utm</i></td><td>Log traffic that has a security profile applied to it.</td></tr><tr><td><i>disable</i></td><td>Disable all logging for this policy.</td></tr></table>	Option	Description	<i>all</i>	Log all sessions accepted or denied by this policy.	<i>utm</i>	Log traffic that has a security profile applied to it.	<i>disable</i>	Disable all logging for this policy.			
Option	Description											
<i>all</i>	Log all sessions accepted or denied by this policy.											
<i>utm</i>	Log traffic that has a security profile applied to it.											
<i>disable</i>	Disable all logging for this policy.											
max-packet-count	Maximum packet count.	integer	Minimum value: 1 Maximum value: 1000000 **	4000								
non-ip	Enable/disable sniffing non-IP packets.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable sniffer for non-IP packets.</td></tr><tr><td><i>disable</i></td><td>Disable sniffer for non-IP packets.</td></tr></table>	Option	Description	<i>enable</i>	Enable sniffer for non-IP packets.	<i>disable</i>	Disable sniffer for non-IP packets.					
Option	Description											
<i>enable</i>	Enable sniffer for non-IP packets.											
<i>disable</i>	Disable sniffer for non-IP packets.											

Parameter	Description	Type	Size	Default
port	Ports to sniff.	string	Maximum length: 63	
protocol	Integer value for the protocol type as defined by IANA.	string	Maximum length: 63	
status	Enable/disable the active status of the sniffer.	option	-	enable
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Enable sniffer status.		
	<i>disable</i>	Disable sniffer status.		
vlan	List of VLANs to sniff.	string	Maximum length: 63	
webfilter-profile	Name of an existing web filter profile.	string	Maximum length: 35	
webfilter-profile-status	Enable/disable web filter profile.	option	-	disable
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

\*\* Values may differ between models.

## config anomaly

Parameter	Description	Type	Size	Default
name	Anomaly name.	string	Maximum length: 63	
status	Enable/disable this anomaly.	option	-	disable
	<b>Option</b> <b>Description</b>			
	<i>disable</i>	Disable this status.		
	<i>enable</i>	Enable this status.		
log	Enable/disable anomaly logging.	option	-	disable
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Enable anomaly logging.		
	<i>disable</i>	Disable anomaly logging.		

Parameter	Description	Type	Size	Default
action	Action taken when the threshold is reached.	option	-	pass
	<b>Option</b>	<b>Description</b>		
	<i>pass</i>	Allow traffic but record a log message if logging is enabled.		
	<i>block</i>	Block traffic if this anomaly is found.		
quarantine	Quarantine method.	option	-	none
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	Quarantine is disabled.		
	<i>attacker</i>	Block all traffic sent from attacker's IP address. The attacker's IP address is also added to the banned user list. The target's address is not affected.		
quarantine-expiry	Duration of quarantine.. Requires quarantine set to attacker.	user	Not Specified	5m
quarantine-log	Enable/disable quarantine logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable quarantine logging.		
	<i>enable</i>	Enable quarantine logging.		
threshold	Anomaly threshold. Number of detected instances (packets per second or concurrent session number) that triggers the anomaly action.	integer	Minimum value: 1 Maximum value: 2147483647	0
threshold (default)	Number of detected instances. Note that each anomaly has a different threshold value assigned to it.	integer	Minimum value: 0 Maximum value: 4294967295	0

## config firewall ssh host-key

SSH proxy host public keys.

```
config firewall ssh host-key
    Description: SSH proxy host public keys.
    edit <name>
        set hostname {string}
        set ip {ipv4-address-any}
        set nid [256|384|...]
        set port {integer}
```

```

    set public-key {var-string}
    set status [trusted|revoked]
    set type [RSA|DSA|...]
    set usage [transparent-proxy|access-proxy]
next
end

```

## config firewall ssh host-key

Parameter	Description	Type	Size	Default								
hostname	Hostname of the SSH server to match SSH certificate principals.	string	Maximum length: 255									
ip	IP address of the SSH server.	ipv4-address-any	Not Specified	0.0.0.0								
name	SSH public key name.	string	Maximum length: 35									
nid	Set the nid of the ECDSA key.	option	-	256								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>256</td><td>The NID is ecdsa-sha2-nistp256.</td></tr><tr><td>384</td><td>The NID is ecdsa-sha2-nistp384.</td></tr><tr><td>521</td><td>The NID is ecdsa-sha2-nistp521.</td></tr></table>				Option	Description	256	The NID is ecdsa-sha2-nistp256.	384	The NID is ecdsa-sha2-nistp384.	521	The NID is ecdsa-sha2-nistp521.
Option	Description											
256	The NID is ecdsa-sha2-nistp256.											
384	The NID is ecdsa-sha2-nistp384.											
521	The NID is ecdsa-sha2-nistp521.											
port	Port of the SSH server.	integer	Minimum value: 0 Maximum value: 4294967295	22								
public-key	SSH public key.	var-string	Maximum length: 32768									
status	Set the trust status of the public key.	option	-	trusted								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>trusted</td><td>The public key is trusted.</td></tr><tr><td>revoked</td><td>The public key is revoked.</td></tr></table>				Option	Description	trusted	The public key is trusted.	revoked	The public key is revoked.		
Option	Description											
trusted	The public key is trusted.											
revoked	The public key is revoked.											
type	Set the type of the public key.	option	-	RSA								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>RSA</td><td>The type of the public key is RSA.</td></tr></table>				Option	Description	RSA	The type of the public key is RSA.				
Option	Description											
RSA	The type of the public key is RSA.											

Parameter	Description	Type	Size	Default																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>DSA</td><td>The type of the public key is DSA.</td></tr><tr><td>ECDSA</td><td>The type of the public key is ECDSA.</td></tr><tr><td>ED25519</td><td>The type of the public key is ED25519.</td></tr><tr><td>RSA-CA</td><td>The type of the public key is from RSA CA.</td></tr><tr><td>DSA-CA</td><td>The type of the public key is from DSA CA.</td></tr><tr><td>ECDSA-CA</td><td>The type of the public key is from ECDSA CA.</td></tr><tr><td>ED25519-CA</td><td>The type of the public key is from ED25519 CA.</td></tr></table>	Option	Description	DSA	The type of the public key is DSA.	ECDSA	The type of the public key is ECDSA.	ED25519	The type of the public key is ED25519.	RSA-CA	The type of the public key is from RSA CA.	DSA-CA	The type of the public key is from DSA CA.	ECDSA-CA	The type of the public key is from ECDSA CA.	ED25519-CA	The type of the public key is from ED25519 CA.			
	Option	Description																		
	DSA	The type of the public key is DSA.																		
	ECDSA	The type of the public key is ECDSA.																		
	ED25519	The type of the public key is ED25519.																		
	RSA-CA	The type of the public key is from RSA CA.																		
	DSA-CA	The type of the public key is from DSA CA.																		
	ECDSA-CA	The type of the public key is from ECDSA CA.																		
ED25519-CA	The type of the public key is from ED25519 CA.																			
usage	Usage for this public key.	option	-	transparent-proxy																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>transparent-proxy</td><td>Transparent proxy uses this public key to validate server.</td></tr><tr><td>access-proxy</td><td>Access proxy uses this public key to validate server.</td></tr></table>	Option	Description	transparent-proxy	Transparent proxy uses this public key to validate server.	access-proxy	Access proxy uses this public key to validate server.													
	Option	Description																		
	transparent-proxy	Transparent proxy uses this public key to validate server.																		
access-proxy	Access proxy uses this public key to validate server.																			

## config firewall ssh local-ca

SSH proxy local CA.

```
config firewall ssh local-ca
  Description: SSH proxy local CA.
  edit <name>
    set password {password}
    set private-key {user}
    set public-key {user}
    set source [built-in|user]
  next
end
```

## config firewall ssh local-ca

Parameter	Description	Type	Size	Default
name	SSH proxy local CA name.	string	Maximum length: 35	
password	Password for SSH private key.	password	Not Specified	



Parameter	Description	Type	Size	Default
private-key	SSH proxy private key, encrypted with a password.	user	Not Specified	
public-key	SSH proxy public key.	user	Not Specified	
source	SSH proxy local CA source type.	option	-	user
	Option	Description		
	<i>built-in</i>	Built-in SSH proxy local keys.		
	<i>user</i>	User imported SSH proxy local keys.		

## config firewall ssh local-key

SSH proxy local keys.

```
config firewall ssh local-key
    Description: SSH proxy local keys.
    edit <name>
        set password {password}
        set private-key {user}
        set public-key {user}
        set source [built-in|user]
    next
end
```

## config firewall ssh local-key

Parameter	Description	Type	Size	Default
name	SSH proxy local key name.	string	Maximum length: 35	
password	Password for SSH private key.	password	Not Specified	
private-key	SSH proxy private key, encrypted with a password.	user	Not Specified	
public-key	SSH proxy public key.	user	Not Specified	
source	SSH proxy local key source type.	option	-	user
	Option	Description		
	<i>built-in</i>	Built-in SSH proxy local keys.		
	<i>user</i>	User imported SSH proxy local keys.		

## config firewall ssh setting

SSH proxy settings.

```
config firewall ssh setting
    Description: SSH proxy settings.
    set caname {string}
    set host-trusted-checking [enable|disable]
    set hostkey-dsa1024 {string}
    set hostkey-ecdsa256 {string}
    set hostkey-ecdsa384 {string}
    set hostkey-ecdsa521 {string}
    set hostkey-ed25519 {string}
    set hostkey-rsa2048 {string}
    set untrusted-caname {string}
end
```

## config firewall ssh setting

Parameter	Description	Type	Size	Default
caname	CA certificate used by SSH Inspection.	string	Maximum length: 35	
host-trusted-checking	Enable/disable host trusted checking.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable host key trusted checking.		
	<i>disable</i>	Disable host key trusted checking.		
hostkey-dsa1024	DSA certificate used by SSH proxy.	string	Maximum length: 35	
hostkey-ecdsa256	ECDSA nid256 certificate used by SSH proxy.	string	Maximum length: 35	
hostkey-ecdsa384	ECDSA nid384 certificate used by SSH proxy.	string	Maximum length: 35	
hostkey-ecdsa521	ECDSA nid384 certificate used by SSH proxy.	string	Maximum length: 35	
hostkey-ed25519	ED25519 hostkey used by SSH proxy.	string	Maximum length: 35	
hostkey-rsa2048	RSA certificate used by SSH proxy.	string	Maximum length: 35	
untrusted-caname	Untrusted CA certificate used by SSH Inspection.	string	Maximum length: 35	

## config firewall ssl-server

Configure SSL servers.

```
config firewall ssl-server
  Description: Configure SSL servers.
  edit <name>
    set add-header-x-forwarded-proto [enable|disable]
    set ip {ipv4-address-any}
    set mapped-port {integer}
    set port {integer}
    set ssl-algorithm [high|medium|...]
    set ssl-cert {string}
    set ssl-client-renegotiation [allow|deny|...]
    set ssl-dh-bits [768|1024|...]
    set ssl-max-version [tls-1.0|tls-1.1|...]
    set ssl-min-version [tls-1.0|tls-1.1|...]
    set ssl-mode [half|full]
    set ssl-send-empty-frags [enable|disable]
    set url-rewrite [enable|disable]
  next
end
```

## config firewall ssl-server

Parameter	Description	Type	Size	Default
add-header-x-forwarded-proto	Enable/disable adding an X-Forwarded-Proto header to forwarded requests.	option	-	enable
		<b>Option</b>	<b>Description</b>	
		<i>enable</i>	Add X-Forwarded-Proto header.	
		<i>disable</i>	Do not add X-Forwarded-Proto header.	
ip	IPv4 address of the SSL server.	ipv4-address-any	Not Specified	0.0.0.0
mapped-port	Mapped server service port.	integer	Minimum value: 1 Maximum value: 65535	80
name	Server name.	string	Maximum length: 35	

Parameter	Description	Type	Size	Default										
port	Server service port.	integer	Minimum value: 1 Maximum value: 65535	443										
ssl-algorithm	Relative strength of encryption algorithms accepted in negotiation.	option	-	high										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>high</i></td><td>High encryption. Allow only AES and ChaCha</td></tr><tr><td><i>medium</i></td><td>Medium encryption. Allow AES, ChaCha, 3DES, and RC4.</td></tr><tr><td><i>low</i></td><td>Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.</td></tr></table>	Option	Description	<i>high</i>	High encryption. Allow only AES and ChaCha	<i>medium</i>	Medium encryption. Allow AES, ChaCha, 3DES, and RC4.	<i>low</i>	Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.					
Option	Description													
<i>high</i>	High encryption. Allow only AES and ChaCha													
<i>medium</i>	Medium encryption. Allow AES, ChaCha, 3DES, and RC4.													
<i>low</i>	Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.													
ssl-cert	Name of certificate for SSL connections to this server.	string	Maximum length: 35	Fortinet_CA_SSL										
ssl-client-renegotiation	Allow or block client renegotiation by server.	option	-	allow										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow a SSL client to renegotiate.</td></tr><tr><td><i>deny</i></td><td>Abort any SSL connection that attempts to renegotiate.</td></tr><tr><td><i>secure</i></td><td>Reject any SSL connection that does not offer a RFC 5746 Secure Renegotiation Indication.</td></tr></table>	Option	Description	<i>allow</i>	Allow a SSL client to renegotiate.	<i>deny</i>	Abort any SSL connection that attempts to renegotiate.	<i>secure</i>	Reject any SSL connection that does not offer a RFC 5746 Secure Renegotiation Indication.					
Option	Description													
<i>allow</i>	Allow a SSL client to renegotiate.													
<i>deny</i>	Abort any SSL connection that attempts to renegotiate.													
<i>secure</i>	Reject any SSL connection that does not offer a RFC 5746 Secure Renegotiation Indication.													
ssl-dh-bits	Bit-size of Diffie-Hellman.	option	-	2048										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>768</i></td><td>768-bit Diffie-Hellman prime.</td></tr><tr><td><i>1024</i></td><td>1024-bit Diffie-Hellman prime.</td></tr><tr><td><i>1536</i></td><td>1536-bit Diffie-Hellman prime.</td></tr><tr><td><i>2048</i></td><td>2048-bit Diffie-Hellman prime.</td></tr></table>	Option	Description	<i>768</i>	768-bit Diffie-Hellman prime.	<i>1024</i>	1024-bit Diffie-Hellman prime.	<i>1536</i>	1536-bit Diffie-Hellman prime.	<i>2048</i>	2048-bit Diffie-Hellman prime.			
Option	Description													
<i>768</i>	768-bit Diffie-Hellman prime.													
<i>1024</i>	1024-bit Diffie-Hellman prime.													
<i>1536</i>	1536-bit Diffie-Hellman prime.													
<i>2048</i>	2048-bit Diffie-Hellman prime.													
ssl-max-version	Highest SSL/TLS version to negotiate.	option	-	tls-1.3										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>tls-1.0</i></td><td>TLS 1.0.</td></tr><tr><td><i>tls-1.1</i></td><td>TLS 1.1.</td></tr></table>	Option	Description	<i>tls-1.0</i>	TLS 1.0.	<i>tls-1.1</i>	TLS 1.1.							
Option	Description													
<i>tls-1.0</i>	TLS 1.0.													
<i>tls-1.1</i>	TLS 1.1.													

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>tls-1.2</i>	TLS 1.2.		
	<i>tls-1.3</i>	TLS 1.3.		
ssl-min-version	Lowest SSL/TLS version to negotiate.	option	-	tls-1.1
	<b>Option</b>	<b>Description</b>		
	<i>tls-1.0</i>	TLS 1.0.		
	<i>tls-1.1</i>	TLS 1.1.		
	<i>tls-1.2</i>	TLS 1.2.		
	<i>tls-1.3</i>	TLS 1.3.		
ssl-mode	SSL/TLS mode for encryption and decryption of traffic.	option	-	full
	<b>Option</b>	<b>Description</b>		
	<i>half</i>	Client to FortiGate SSL.		
	<i>full</i>	Client to FortiGate and FortiGate to Server SSL.		
ssl-send-empty-frags	Enable/disable sending empty fragments to avoid attack on CBC IV.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Send empty fragments.		
	<i>disable</i>	Do not send empty fragments.		
url-rewrite	Enable/disable rewriting the URL.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

## config firewall ssl-ssh-profile

Configure SSL/SSH protocol options.

```
config firewall ssl-ssh-profile
  Description: Configure SSL/SSH protocol options.
  edit <name>
    set allowlist [enable|disable]
    set block-blocklisted-certificates [disable|enable]
    set caname {string}
    set comment {var-string}
```

```

config dot
    Description: Configure DNS over TLS options.
    set status [disable|deep-inspection]
    set proxy-after-tcp-handshake [enable|disable]
    set client-certificate [bypass|inspect|...]
    set unsupported-ssl-version [allow|block]
    set unsupported-ssl-cipher [allow|block]
    set unsupported-ssl-negotiation [allow|block]
    set expired-server-cert [allow|block|...]
    set revoked-server-cert [allow|block|...]
    set untrusted-server-cert [allow|block|...]
    set cert-validation-timeout [allow|block|...]
    set cert-validation-failure [allow|block|...]
    set sni-server-cert-check [enable|strict|...]
end
config ftps
    Description: Configure FTPS options.
    set ports {integer}
    set status [disable|deep-inspection]
    set client-certificate [bypass|inspect|...]
    set unsupported-ssl-version [allow|block]
    set unsupported-ssl-cipher [allow|block]
    set unsupported-ssl-negotiation [allow|block]
    set expired-server-cert [allow|block|...]
    set revoked-server-cert [allow|block|...]
    set untrusted-server-cert [allow|block|...]
    set cert-validation-timeout [allow|block|...]
    set cert-validation-failure [allow|block|...]
    set sni-server-cert-check [enable|strict|...]
    set min-allowed-ssl-version [ssl-3.0|tls-1.0|...]
end
config https
    Description: Configure HTTPS options.
    set ports {integer}
    set status [disable|certificate-inspection|...]
    set proxy-after-tcp-handshake [enable|disable]
    set client-certificate [bypass|inspect|...]
    set unsupported-ssl-version [allow|block]
    set unsupported-ssl-cipher [allow|block]
    set unsupported-ssl-negotiation [allow|block]
    set expired-server-cert [allow|block|...]
    set revoked-server-cert [allow|block|...]
    set untrusted-server-cert [allow|block|...]
    set cert-validation-timeout [allow|block|...]
    set cert-validation-failure [allow|block|...]
    set sni-server-cert-check [enable|strict|...]
    set cert-probe-failure [allow|block]
    set min-allowed-ssl-version [ssl-3.0|tls-1.0|...]
end
config imaps
    Description: Configure IMAPS options.
    set ports {integer}
    set status [disable|deep-inspection]
    set proxy-after-tcp-handshake [enable|disable]
    set client-certificate [bypass|inspect|...]
    set unsupported-ssl-version [allow|block]

```

```

    set unsupported-ssl-cipher [allow|block]
    set unsupported-ssl-negotiation [allow|block]
    set expired-server-cert [allow|block|...]
    set revoked-server-cert [allow|block|...]
    set untrusted-server-cert [allow|block|...]
    set cert-validation-timeout [allow|block|...]
    set cert-validation-failure [allow|block|...]
    set sni-server-cert-check [enable|strict|...]
end
set mapi-over-https [enable|disable]
config pop3s
    Description: Configure POP3S options.
    set ports {integer}
    set status [disable|deep-inspection]
    set proxy-after-tcp-handshake [enable|disable]
    set client-certificate [bypass|inspect|...]
    set unsupported-ssl-version [allow|block]
    set unsupported-ssl-cipher [allow|block]
    set unsupported-ssl-negotiation [allow|block]
    set expired-server-cert [allow|block|...]
    set revoked-server-cert [allow|block|...]
    set untrusted-server-cert [allow|block|...]
    set cert-validation-timeout [allow|block|...]
    set cert-validation-failure [allow|block|...]
    set sni-server-cert-check [enable|strict|...]
end
set rpc-over-https [enable|disable]
set server-cert <name1>, <name2>, ...
set server-cert-mode [re-sign|replace]
config smtps
    Description: Configure SMTPS options.
    set ports {integer}
    set status [disable|deep-inspection]
    set proxy-after-tcp-handshake [enable|disable]
    set client-certificate [bypass|inspect|...]
    set unsupported-ssl-version [allow|block]
    set unsupported-ssl-cipher [allow|block]
    set unsupported-ssl-negotiation [allow|block]
    set expired-server-cert [allow|block|...]
    set revoked-server-cert [allow|block|...]
    set untrusted-server-cert [allow|block|...]
    set cert-validation-timeout [allow|block|...]
    set cert-validation-failure [allow|block|...]
    set sni-server-cert-check [enable|strict|...]
end
config ssh
    Description: Configure SSH options.
    set ports {integer}
    set status [disable|deep-inspection]
    set inspect-all [disable|deep-inspection]
    set proxy-after-tcp-handshake [enable|disable]
    set unsupported-version [bypass|block]
    set ssh-tun-policy-check [disable|enable]
    set ssh-algorithm [compatible|high-encryption]
end
config ssl

```

```

Description: Configure SSL options.
set inspect-all [disable|certificate-inspection|...]
set client-certificate [bypass|inspect|...]
set unsupported-ssl-version [allow|block]
set unsupported-ssl-cipher [allow|block]
set unsupported-ssl-negotiation [allow|block]
set expired-server-cert [allow|block|...]
set revoked-server-cert [allow|block|...]
set untrusted-server-cert [allow|block|...]
set cert-validation-timeout [allow|block|...]
set cert-validation-failure [allow|block|...]
set sni-server-cert-check [enable|strict|...]
set cert-probe-failure [allow|block]
set min-allowed-ssl-version [ssl-3.0|tls-1.0|...]
end
set ssl-anomaly-log [disable|enable]
config ssl-exempt
Description: Servers to exempt from SSL inspection.
edit <id>
    set type [fortiguard-category|address|...]
    set fortiguard-category {integer}
    set address {string}
    set address6 {string}
    set wildcard-fqdn {string}
    set regex {string}
next
end
set ssl-exemption-ip-rating [enable|disable]
set ssl-exemption-log [disable|enable]
set ssl-handshake-log [disable|enable]
set ssl-negotiation-log [disable|enable]
config ssl-server
Description: SSL server settings used for client certificate request.
edit <id>
    set ip {ipv4-address-any}
    set https-client-certificate [bypass|inspect|...]
    set smtps-client-certificate [bypass|inspect|...]
    set pop3s-client-certificate [bypass|inspect|...]
    set imaps-client-certificate [bypass|inspect|...]
    set ftps-client-certificate [bypass|inspect|...]
    set ssl-other-client-certificate [bypass|inspect|...]
next
end
set ssl-server-cert-log [disable|enable]
set supported-alpn [http1-1|http2|...]
set untrusted-caname {string}
set use-ssl-server [disable|enable]
next
end

```



## config firewall ssl-ssh-profile

Parameter	Description	Type	Size	Default						
allowlist	Enable/disable exempting servers by FortiGuard allowlist.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
block-blocklisted-certificates	Enable/disable blocking SSL-based botnet communication by FortiGuard certificate blocklist.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable FortiGuard certificate blocklist.</td></tr><tr><td><i>enable</i></td><td>Enable FortiGuard certificate blocklist.</td></tr></table>	Option	Description	<i>disable</i>	Disable FortiGuard certificate blocklist.	<i>enable</i>	Enable FortiGuard certificate blocklist.			
Option	Description									
<i>disable</i>	Disable FortiGuard certificate blocklist.									
<i>enable</i>	Enable FortiGuard certificate blocklist.									
caname	CA certificate used by SSL Inspection.	string	Maximum length: 35	Fortinet_CA_SSL						
comment	Optional comments.	var-string	Maximum length: 255							
mapi-over-https	Enable/disable inspection of MAPI over HTTPS.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable inspection of MAPI over HTTPS.</td></tr><tr><td><i>disable</i></td><td>Disable inspection of MAPI over HTTPS.</td></tr></table>	Option	Description	<i>enable</i>	Enable inspection of MAPI over HTTPS.	<i>disable</i>	Disable inspection of MAPI over HTTPS.			
Option	Description									
<i>enable</i>	Enable inspection of MAPI over HTTPS.									
<i>disable</i>	Disable inspection of MAPI over HTTPS.									
name	Name.	string	Maximum length: 35							
rpc-over-https	Enable/disable inspection of RPC over HTTPS.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable inspection of RPC over HTTPS.</td></tr><tr><td><i>disable</i></td><td>Disable inspection of RPC over HTTPS.</td></tr></table>	Option	Description	<i>enable</i>	Enable inspection of RPC over HTTPS.	<i>disable</i>	Disable inspection of RPC over HTTPS.			
Option	Description									
<i>enable</i>	Enable inspection of RPC over HTTPS.									
<i>disable</i>	Disable inspection of RPC over HTTPS.									
server-cert <name>	Certificate used by SSL Inspection to replace server certificate. Certificate list.	string	Maximum length: 35							
server-cert-mode	Re-sign or replace the server's certificate.	option	-	re-sign						

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>re-sign</i>	Multiple clients connecting to multiple servers.		
	<i>replace</i>	Protect an SSL server.		
ssl-anomaly-log	Enable/disable logging of SSL anomalies.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable logging of SSL anomalies.		
	<i>enable</i>	Enable logging of SSL anomalies.		
ssl-exemption-ip-rating	Enable/disable IP based URL rating.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable IP based URL rating.		
	<i>disable</i>	Disable IP based URL rating.		
ssl-exemption-log	Enable/disable logging SSL exemptions.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable logging SSL exemptions.		
	<i>enable</i>	Enable logging SSL exemptions.		
ssl-handshake-log	Enable/disable logging of TLS handshakes.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable logging TLS handshakes.		
	<i>enable</i>	Enable logging TLS handshakes.		
ssl-negotiation-log	Enable/disable logging SSL negotiation.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable logging SSL negotiation.		
	<i>enable</i>	Enable logging SSL negotiation.		

Parameter	Description	Type	Size	Default										
ssl-server-cert-log	Enable/disable logging of server certificate information.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable logging server certificate.</td></tr><tr><td>enable</td><td>Enable logging server certificate.</td></tr></table>	Option	Description	disable	Disable logging server certificate.	enable	Enable logging server certificate.							
Option	Description													
disable	Disable logging server certificate.													
enable	Enable logging server certificate.													
supported-alpn	Configure ALPN option.	option	-	all										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>http1-1</td><td>Enable ALPN of HTTP1.1.</td></tr><tr><td>http2</td><td>Enable ALPN of HTTP2.</td></tr><tr><td>all</td><td>Enable ALPN of HTTP1.1 and HTTP2.</td></tr><tr><td>none</td><td>Do not use ALPN.</td></tr></table>	Option	Description	http1-1	Enable ALPN of HTTP1.1.	http2	Enable ALPN of HTTP2.	all	Enable ALPN of HTTP1.1 and HTTP2.	none	Do not use ALPN.			
Option	Description													
http1-1	Enable ALPN of HTTP1.1.													
http2	Enable ALPN of HTTP2.													
all	Enable ALPN of HTTP1.1 and HTTP2.													
none	Do not use ALPN.													
untrusted-caname	Untrusted CA certificate used by SSL Inspection.	string	Maximum length: 35	Fortinet_CA_Untrusted										
use-ssl-server	Enable/disable the use of SSL server table for SSL offloading.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Don't use SSL server configuration.</td></tr><tr><td>enable</td><td>Use SSL server configuration.</td></tr></table>	Option	Description	disable	Don't use SSL server configuration.	enable	Use SSL server configuration.							
Option	Description													
disable	Don't use SSL server configuration.													
enable	Use SSL server configuration.													

## config dot

Parameter	Description	Type	Size	Default
status	Configure protocol inspection status.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable.		
	<i>deep-inspection</i>	Full SSL inspection.		
proxy-after-tcp-handshake	Proxy traffic after the TCP 3-way handshake has been established (not before).	option	-	disable

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
client-certificate	Action based on received client certificate.	option	-	bypass
	<b>Option</b>	<b>Description</b>		
	<i>bypass</i>	Bypass the session.		
	<i>inspect</i>	Inspect the session.		
	<i>block</i>	Block the session.		
unsupported-ssl-version	Action based on the SSL version used being unsupported.	option	-	block
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Bypass the session when the version is not supported.		
	<i>block</i>	Block the session when the version is not supported.		
unsupported-ssl-cipher	Action based on the SSL cipher used being unsupported.	option	-	allow
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Bypass the session when the cipher is not supported.		
	<i>block</i>	Block the session when the cipher is not supported.		
unsupported-ssl-negotiation	Action based on the SSL negotiation used being unsupported.	option	-	allow
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Bypass the session when the negotiation is not supported.		
	<i>block</i>	Block the session when the negotiation is not supported.		
expired-server-cert	Action based on server certificate is expired.	option	-	block
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow the server certificate.		
	<i>block</i>	Block the session.		
	<i>ignore</i>	Re-sign the server certificate as trusted.		

Parameter	Description	Type	Size	Default								
revoked-server-cert	Action based on server certificate is revoked.	option	-	block								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow the server certificate.</td></tr><tr><td><i>block</i></td><td>Block the session.</td></tr><tr><td><i>ignore</i></td><td>Re-sign the server certificate as trusted.</td></tr></table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
Option	Description											
<i>allow</i>	Allow the server certificate.											
<i>block</i>	Block the session.											
<i>ignore</i>	Re-sign the server certificate as trusted.											
untrusted-server-cert	Action based on server certificate is not issued by a trusted CA.	option	-	allow								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow the server certificate.</td></tr><tr><td><i>block</i></td><td>Block the session.</td></tr><tr><td><i>ignore</i></td><td>Re-sign the server certificate as trusted.</td></tr></table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
Option	Description											
<i>allow</i>	Allow the server certificate.											
<i>block</i>	Block the session.											
<i>ignore</i>	Re-sign the server certificate as trusted.											
cert-validation-timeout	Action based on certificate validation timeout.	option	-	allow								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow the server certificate.</td></tr><tr><td><i>block</i></td><td>Block the session.</td></tr><tr><td><i>ignore</i></td><td>Re-sign the server certificate as trusted.</td></tr></table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
Option	Description											
<i>allow</i>	Allow the server certificate.											
<i>block</i>	Block the session.											
<i>ignore</i>	Re-sign the server certificate as trusted.											
cert-validation-failure	Action based on certificate validation failure.	option	-	block								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow the server certificate.</td></tr><tr><td><i>block</i></td><td>Block the session.</td></tr><tr><td><i>ignore</i></td><td>Re-sign the server certificate as trusted.</td></tr></table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
Option	Description											
<i>allow</i>	Allow the server certificate.											
<i>block</i>	Block the session.											
<i>ignore</i>	Re-sign the server certificate as trusted.											
sni-server-cert-check	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.</td></tr></table>	Option	Description	<i>enable</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.							
Option	Description											
<i>enable</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.											

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>strict</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.		
	<i>disable</i>	Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.		

## config ftps

Parameter	Description	Type	Size	Default
ports	Ports to use for scanning.	integer	Minimum value: 1 Maximum value: 65535	
status	Configure protocol inspection status.	option	-	deep-inspection
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable.		
	<i>deep-inspection</i>	Full SSL inspection.		
client-certificate	Action based on received client certificate.	option	-	bypass
	<b>Option</b>	<b>Description</b>		
	<i>bypass</i>	Bypass the session.		
	<i>inspect</i>	Inspect the session.		
	<i>block</i>	Block the session.		
unsupported-ssl-version	Action based on the SSL version used being unsupported.	option	-	block
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Bypass the session when the version is not supported.		
	<i>block</i>	Block the session when the version is not supported.		
unsupported-ssl-cipher	Action based on the SSL cipher used being unsupported.	option	-	allow

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Bypass the session when the cipher is not supported.		
	<i>block</i>	Block the session when the cipher is not supported.		
unsupported-ssl-negotiation	Action based on the SSL negotiation used being unsupported.	option	-	allow
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Bypass the session when the negotiation is not supported.		
	<i>block</i>	Block the session when the negotiation is not supported.		
expired-server-cert	Action based on server certificate is expired.	option	-	block
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow the server certificate.		
	<i>block</i>	Block the session.		
	<i>ignore</i>	Re-sign the server certificate as trusted.		
revoked-server-cert	Action based on server certificate is revoked.	option	-	block
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow the server certificate.		
	<i>block</i>	Block the session.		
	<i>ignore</i>	Re-sign the server certificate as trusted.		
untrusted-server-cert	Action based on server certificate is not issued by a trusted CA.	option	-	allow
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow the server certificate.		
	<i>block</i>	Block the session.		
	<i>ignore</i>	Re-sign the server certificate as trusted.		
cert-validation-timeout	Action based on certificate validation timeout.	option	-	allow

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow the server certificate.		
	<i>block</i>	Block the session.		
	<i>ignore</i>	Re-sign the server certificate as trusted.		
cert-validation-failure	Action based on certificate validation failure.	option	-	block
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow the server certificate.		
	<i>block</i>	Block the session.		
	<i>ignore</i>	Re-sign the server certificate as trusted.		
sni-server-cert-check	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.		
	<i>strict</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.		
	<i>disable</i>	Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.		
min-allowed-ssl-version	Minimum SSL version to be allowed. Flow-based inspection does not support SSL version control.	option	-	tls-1.1
	<b>Option</b>	<b>Description</b>		
	<i>ssl-3.0</i>	SSL 3.0.		
	<i>tls-1.0</i>	TLS 1.0.		
	<i>tls-1.1</i>	TLS 1.1.		
	<i>tls-1.2</i>	TLS 1.2.		
	<i>tls-1.3</i>	TLS 1.3.		



## config https

Parameter	Description	Type	Size	Default								
ports	Ports to use for scanning.	integer	Minimum value: 1 Maximum value: 65535									
status	Configure protocol inspection status.	option	-	deep-inspection								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable.</td></tr><tr><td><i>certificate-inspection</i></td><td>Inspect SSL handshake only.</td></tr><tr><td><i>deep-inspection</i></td><td>Full SSL inspection.</td></tr></table>	Option	Description	<i>disable</i>	Disable.	<i>certificate-inspection</i>	Inspect SSL handshake only.	<i>deep-inspection</i>	Full SSL inspection.			
Option	Description											
<i>disable</i>	Disable.											
<i>certificate-inspection</i>	Inspect SSL handshake only.											
<i>deep-inspection</i>	Full SSL inspection.											
proxy-after-tcp-handshake	Proxy traffic after the TCP 3-way handshake has been established (not before).	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
client-certificate	Action based on received client certificate.	option	-	bypass								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>bypass</i></td><td>Bypass the session.</td></tr><tr><td><i>inspect</i></td><td>Inspect the session.</td></tr><tr><td><i>block</i></td><td>Block the session.</td></tr></table>	Option	Description	<i>bypass</i>	Bypass the session.	<i>inspect</i>	Inspect the session.	<i>block</i>	Block the session.			
Option	Description											
<i>bypass</i>	Bypass the session.											
<i>inspect</i>	Inspect the session.											
<i>block</i>	Block the session.											
unsupported-ssl-version	Action based on the SSL version used being unsupported.	option	-	block								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Bypass the session when the version is not supported.</td></tr><tr><td><i>block</i></td><td>Block the session when the version is not supported.</td></tr></table>	Option	Description	<i>allow</i>	Bypass the session when the version is not supported.	<i>block</i>	Block the session when the version is not supported.					
Option	Description											
<i>allow</i>	Bypass the session when the version is not supported.											
<i>block</i>	Block the session when the version is not supported.											
unsupported-ssl-cipher	Action based on the SSL cipher used being unsupported.	option	-	allow								

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Bypass the session when the cipher is not supported.		
	<i>block</i>	Block the session when the cipher is not supported.		
unsupported-ssl-negotiation	Action based on the SSL negotiation used being unsupported.	option	-	allow
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Bypass the session when the negotiation is not supported.		
	<i>block</i>	Block the session when the negotiation is not supported.		
expired-server-cert	Action based on server certificate is expired.	option	-	block
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow the server certificate.		
	<i>block</i>	Block the session.		
	<i>ignore</i>	Re-sign the server certificate as trusted.		
revoked-server-cert	Action based on server certificate is revoked.	option	-	block
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow the server certificate.		
	<i>block</i>	Block the session.		
	<i>ignore</i>	Re-sign the server certificate as trusted.		
untrusted-server-cert	Action based on server certificate is not issued by a trusted CA.	option	-	allow
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow the server certificate.		
	<i>block</i>	Block the session.		
	<i>ignore</i>	Re-sign the server certificate as trusted.		
cert-validation-timeout	Action based on certificate validation timeout.	option	-	allow

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow the server certificate.		
	<i>block</i>	Block the session.		
	<i>ignore</i>	Re-sign the server certificate as trusted.		
cert-validation-failure	Action based on certificate validation failure.	option	-	block
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow the server certificate.		
	<i>block</i>	Block the session.		
	<i>ignore</i>	Re-sign the server certificate as trusted.		
sni-server-cert-check	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.		
	<i>strict</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.		
	<i>disable</i>	Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.		
cert-probe-failure	Action based on certificate probe failure.	option	-	block
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Bypass the session when unable to retrieve server's certificate for inspection.		
	<i>block</i>	Block the session when unable to retrieve server's certificate for inspection.		
min-allowed-ssl-version	Minimum SSL version to be allowed. Flow-based inspection does not support SSL version control.	option	-	tls-1.1
	<b>Option</b>	<b>Description</b>		
	<i>ssl-3.0</i>	SSL 3.0.		
	<i>tls-1.0</i>	TLS 1.0.		

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>tls-1.1</i>	TLS 1.1.		
	<i>tls-1.2</i>	TLS 1.2.		
	<i>tls-1.3</i>	TLS 1.3.		

## config imaps

Parameter	Description	Type	Size	Default
ports	Ports to use for scanning.	integer	Minimum value: 1 Maximum value: 65535	
status	Configure protocol inspection status.	option	-	deep-inspection
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable.		
	<i>deep-inspection</i>	Full SSL inspection.		
proxy-after-tcp-handshake	Proxy traffic after the TCP 3-way handshake has been established (not before).	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
client-certificate	Action based on received client certificate.	option	-	inspect
	<b>Option</b>	<b>Description</b>		
	<i>bypass</i>	Bypass the session.		
	<i>inspect</i>	Inspect the session.		
	<i>block</i>	Block the session.		
unsupported-ssl-version	Action based on the SSL version used being unsupported.	option	-	block
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Bypass the session when the version is not supported.		

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>block</i>	Block the session when the version is not supported.		
unsupported-ssl-cipher	Action based on the SSL cipher used being unsupported.	option	-	allow
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Bypass the session when the cipher is not supported.		
	<i>block</i>	Block the session when the cipher is not supported.		
unsupported-ssl-negotiation	Action based on the SSL negotiation used being unsupported.	option	-	allow
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Bypass the session when the negotiation is not supported.		
	<i>block</i>	Block the session when the negotiation is not supported.		
expired-server-cert	Action based on server certificate is expired.	option	-	block
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow the server certificate.		
	<i>block</i>	Block the session.		
	<i>ignore</i>	Re-sign the server certificate as trusted.		
revoked-server-cert	Action based on server certificate is revoked.	option	-	block
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow the server certificate.		
	<i>block</i>	Block the session.		
	<i>ignore</i>	Re-sign the server certificate as trusted.		
untrusted-server-cert	Action based on server certificate is not issued by a trusted CA.	option	-	allow
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow the server certificate.		
	<i>block</i>	Block the session.		
	<i>ignore</i>	Re-sign the server certificate as trusted.		

Parameter	Description	Type	Size	Default								
cert-validation-timeout	Action based on certificate validation timeout.	option	-	allow								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allow the server certificate.</td></tr><tr><td>block</td><td>Block the session.</td></tr><tr><td>ignore</td><td>Re-sign the server certificate as trusted.</td></tr></table>	Option	Description	allow	Allow the server certificate.	block	Block the session.	ignore	Re-sign the server certificate as trusted.			
Option	Description											
allow	Allow the server certificate.											
block	Block the session.											
ignore	Re-sign the server certificate as trusted.											
cert-validation-failure	Action based on certificate validation failure.	option	-	block								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allow the server certificate.</td></tr><tr><td>block</td><td>Block the session.</td></tr><tr><td>ignore</td><td>Re-sign the server certificate as trusted.</td></tr></table>	Option	Description	allow	Allow the server certificate.	block	Block the session.	ignore	Re-sign the server certificate as trusted.			
Option	Description											
allow	Allow the server certificate.											
block	Block the session.											
ignore	Re-sign the server certificate as trusted.											
sni-server-cert-check	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.</td></tr><tr><td>strict</td><td>Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.</td></tr><tr><td>disable</td><td>Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.</td></tr></table>	Option	Description	enable	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.	strict	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.	disable	Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.			
Option	Description											
enable	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.											
strict	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.											
disable	Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.											

## config pop3s

Parameter	Description	Type	Size	Default
ports	Ports to use for scanning.	integer	Minimum value: 1 Maximum value: 65535	
status	Configure protocol inspection status.	option	-	deep-inspection

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable.</td></tr><tr><td><i>deep-inspection</i></td><td>Full SSL inspection.</td></tr></table>	Option	Description	<i>disable</i>	Disable.	<i>deep-inspection</i>	Full SSL inspection.					
	Option	Description										
	<i>disable</i>	Disable.										
<i>deep-inspection</i>	Full SSL inspection.											
proxy-after-tcp-handshake	Proxy traffic after the TCP 3-way handshake has been established (not before).	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
	Option	Description										
	<i>enable</i>	Enable setting.										
<i>disable</i>	Disable setting.											
client-certificate	Action based on received client certificate.	option	-	inspect								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>bypass</i></td><td>Bypass the session.</td></tr><tr><td><i>inspect</i></td><td>Inspect the session.</td></tr><tr><td><i>block</i></td><td>Block the session.</td></tr></table>	Option	Description	<i>bypass</i>	Bypass the session.	<i>inspect</i>	Inspect the session.	<i>block</i>	Block the session.			
	Option	Description										
	<i>bypass</i>	Bypass the session.										
	<i>inspect</i>	Inspect the session.										
<i>block</i>	Block the session.											
unsupported-ssl-version	Action based on the SSL version used being unsupported.	option	-	block								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Bypass the session when the version is not supported.</td></tr><tr><td><i>block</i></td><td>Block the session when the version is not supported.</td></tr></table>	Option	Description	<i>allow</i>	Bypass the session when the version is not supported.	<i>block</i>	Block the session when the version is not supported.					
	Option	Description										
	<i>allow</i>	Bypass the session when the version is not supported.										
<i>block</i>	Block the session when the version is not supported.											
unsupported-ssl-cipher	Action based on the SSL cipher used being unsupported.	option	-	allow								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Bypass the session when the cipher is not supported.</td></tr><tr><td><i>block</i></td><td>Block the session when the cipher is not supported.</td></tr></table>	Option	Description	<i>allow</i>	Bypass the session when the cipher is not supported.	<i>block</i>	Block the session when the cipher is not supported.					
	Option	Description										
	<i>allow</i>	Bypass the session when the cipher is not supported.										
<i>block</i>	Block the session when the cipher is not supported.											
unsupported-ssl-negotiation	Action based on the SSL negotiation used being unsupported.	option	-	allow								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Bypass the session when the negotiation is not supported.</td></tr><tr><td><i>block</i></td><td>Block the session when the negotiation is not supported.</td></tr></table>	Option	Description	<i>allow</i>	Bypass the session when the negotiation is not supported.	<i>block</i>	Block the session when the negotiation is not supported.					
	Option	Description										
	<i>allow</i>	Bypass the session when the negotiation is not supported.										
<i>block</i>	Block the session when the negotiation is not supported.											

Parameter	Description	Type	Size	Default								
expired-server-cert	Action based on server certificate is expired.	option	-	block								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow the server certificate.</td></tr><tr><td><i>block</i></td><td>Block the session.</td></tr><tr><td><i>ignore</i></td><td>Re-sign the server certificate as trusted.</td></tr></table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
Option	Description											
<i>allow</i>	Allow the server certificate.											
<i>block</i>	Block the session.											
<i>ignore</i>	Re-sign the server certificate as trusted.											
revoked-server-cert	Action based on server certificate is revoked.	option	-	block								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow the server certificate.</td></tr><tr><td><i>block</i></td><td>Block the session.</td></tr><tr><td><i>ignore</i></td><td>Re-sign the server certificate as trusted.</td></tr></table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
Option	Description											
<i>allow</i>	Allow the server certificate.											
<i>block</i>	Block the session.											
<i>ignore</i>	Re-sign the server certificate as trusted.											
untrusted-server-cert	Action based on server certificate is not issued by a trusted CA.	option	-	allow								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow the server certificate.</td></tr><tr><td><i>block</i></td><td>Block the session.</td></tr><tr><td><i>ignore</i></td><td>Re-sign the server certificate as trusted.</td></tr></table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
Option	Description											
<i>allow</i>	Allow the server certificate.											
<i>block</i>	Block the session.											
<i>ignore</i>	Re-sign the server certificate as trusted.											
cert-validation-timeout	Action based on certificate validation timeout.	option	-	allow								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow the server certificate.</td></tr><tr><td><i>block</i></td><td>Block the session.</td></tr><tr><td><i>ignore</i></td><td>Re-sign the server certificate as trusted.</td></tr></table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
Option	Description											
<i>allow</i>	Allow the server certificate.											
<i>block</i>	Block the session.											
<i>ignore</i>	Re-sign the server certificate as trusted.											
cert-validation-failure	Action based on certificate validation failure.	option	-	block								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow the server certificate.</td></tr><tr><td><i>block</i></td><td>Block the session.</td></tr><tr><td><i>ignore</i></td><td>Re-sign the server certificate as trusted.</td></tr></table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
Option	Description											
<i>allow</i>	Allow the server certificate.											
<i>block</i>	Block the session.											
<i>ignore</i>	Re-sign the server certificate as trusted.											



Parameter	Description	Type	Size	Default								
sni-server-cert-check	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.</td></tr><tr><td><i>strict</i></td><td>Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.</td></tr><tr><td><i>disable</i></td><td>Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.</td></tr></table>	Option	Description	<i>enable</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.	<i>strict</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.	<i>disable</i>	Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.			
Option	Description											
<i>enable</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.											
<i>strict</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.											
<i>disable</i>	Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.											

## config smtps

Parameter	Description	Type	Size	Default								
ports	Ports to use for scanning.	integer	Minimum value: 1 Maximum value: 65535									
status	Configure protocol inspection status.	option	-	deep-inspection								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable.</td></tr><tr><td><i>deep-inspection</i></td><td>Full SSL inspection.</td></tr></table>	Option	Description	<i>disable</i>	Disable.	<i>deep-inspection</i>	Full SSL inspection.					
Option	Description											
<i>disable</i>	Disable.											
<i>deep-inspection</i>	Full SSL inspection.											
proxy-after-tcp-handshake	Proxy traffic after the TCP 3-way handshake has been established (not before).	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
client-certificate	Action based on received client certificate.	option	-	inspect								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>bypass</i></td><td>Bypass the session.</td></tr><tr><td><i>inspect</i></td><td>Inspect the session.</td></tr><tr><td><i>block</i></td><td>Block the session.</td></tr></table>	Option	Description	<i>bypass</i>	Bypass the session.	<i>inspect</i>	Inspect the session.	<i>block</i>	Block the session.			
Option	Description											
<i>bypass</i>	Bypass the session.											
<i>inspect</i>	Inspect the session.											
<i>block</i>	Block the session.											

Parameter	Description	Type	Size	Default								
unsupported-ssl-version	Action based on the SSL version used being unsupported.	option	-	block								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Bypass the session when the version is not supported.</td></tr><tr><td><i>block</i></td><td>Block the session when the version is not supported.</td></tr></table>	Option	Description	<i>allow</i>	Bypass the session when the version is not supported.	<i>block</i>	Block the session when the version is not supported.					
Option	Description											
<i>allow</i>	Bypass the session when the version is not supported.											
<i>block</i>	Block the session when the version is not supported.											
unsupported-ssl-cipher	Action based on the SSL cipher used being unsupported.	option	-	allow								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Bypass the session when the cipher is not supported.</td></tr><tr><td><i>block</i></td><td>Block the session when the cipher is not supported.</td></tr></table>	Option	Description	<i>allow</i>	Bypass the session when the cipher is not supported.	<i>block</i>	Block the session when the cipher is not supported.					
Option	Description											
<i>allow</i>	Bypass the session when the cipher is not supported.											
<i>block</i>	Block the session when the cipher is not supported.											
unsupported-ssl-negotiation	Action based on the SSL negotiation used being unsupported.	option	-	allow								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Bypass the session when the negotiation is not supported.</td></tr><tr><td><i>block</i></td><td>Block the session when the negotiation is not supported.</td></tr></table>	Option	Description	<i>allow</i>	Bypass the session when the negotiation is not supported.	<i>block</i>	Block the session when the negotiation is not supported.					
Option	Description											
<i>allow</i>	Bypass the session when the negotiation is not supported.											
<i>block</i>	Block the session when the negotiation is not supported.											
expired-server-cert	Action based on server certificate is expired.	option	-	block								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow the server certificate.</td></tr><tr><td><i>block</i></td><td>Block the session.</td></tr><tr><td><i>ignore</i></td><td>Re-sign the server certificate as trusted.</td></tr></table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
Option	Description											
<i>allow</i>	Allow the server certificate.											
<i>block</i>	Block the session.											
<i>ignore</i>	Re-sign the server certificate as trusted.											
revoked-server-cert	Action based on server certificate is revoked.	option	-	block								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow the server certificate.</td></tr><tr><td><i>block</i></td><td>Block the session.</td></tr><tr><td><i>ignore</i></td><td>Re-sign the server certificate as trusted.</td></tr></table>	Option	Description	<i>allow</i>	Allow the server certificate.	<i>block</i>	Block the session.	<i>ignore</i>	Re-sign the server certificate as trusted.			
Option	Description											
<i>allow</i>	Allow the server certificate.											
<i>block</i>	Block the session.											
<i>ignore</i>	Re-sign the server certificate as trusted.											
untrusted-server-cert	Action based on server certificate is not issued by a trusted CA.	option	-	allow								

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow the server certificate.		
	<i>block</i>	Block the session.		
	<i>ignore</i>	Re-sign the server certificate as trusted.		
cert-validation-timeout	Action based on certificate validation timeout.	option	-	allow
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow the server certificate.		
	<i>block</i>	Block the session.		
	<i>ignore</i>	Re-sign the server certificate as trusted.		
cert-validation-failure	Action based on certificate validation failure.	option	-	block
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow the server certificate.		
	<i>block</i>	Block the session.		
	<i>ignore</i>	Re-sign the server certificate as trusted.		
sni-server-cert-check	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.		
	<i>strict</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.		
	<i>disable</i>	Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.		

## config ssh

Parameter	Description	Type	Size	Default						
ports	Ports to use for scanning.	integer	Minimum value: 1 Maximum value: 65535							
status	Configure protocol inspection status.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable.</td></tr><tr><td><i>deep-inspection</i></td><td>Full SSL inspection.</td></tr></table>	Option	Description	<i>disable</i>	Disable.	<i>deep-inspection</i>	Full SSL inspection.			
Option	Description									
<i>disable</i>	Disable.									
<i>deep-inspection</i>	Full SSL inspection.									
inspect-all	Level of SSL inspection.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable.</td></tr><tr><td><i>deep-inspection</i></td><td>Full SSL inspection.</td></tr></table>	Option	Description	<i>disable</i>	Disable.	<i>deep-inspection</i>	Full SSL inspection.			
Option	Description									
<i>disable</i>	Disable.									
<i>deep-inspection</i>	Full SSL inspection.									
proxy-after-tcp-handshake	Proxy traffic after the TCP 3-way handshake has been established (not before).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
unsupported-version	Action based on SSH version being unsupported.	option	-	bypass						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>bypass</i></td><td>Bypass the session.</td></tr><tr><td><i>block</i></td><td>Block the session.</td></tr></table>	Option	Description	<i>bypass</i>	Bypass the session.	<i>block</i>	Block the session.			
Option	Description									
<i>bypass</i>	Bypass the session.									
<i>block</i>	Block the session.									
ssh-tun-policy-check	Enable/disable SSH tunnel policy check.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable SSH tunnel policy check.</td></tr><tr><td><i>enable</i></td><td>Enable SSH tunnel policy check.</td></tr></table>	Option	Description	<i>disable</i>	Disable SSH tunnel policy check.	<i>enable</i>	Enable SSH tunnel policy check.			
Option	Description									
<i>disable</i>	Disable SSH tunnel policy check.									
<i>enable</i>	Enable SSH tunnel policy check.									
ssh-algorithm	Relative strength of encryption algorithms accepted during negotiation.	option	-	compatible						

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>compatible</i>	Allow a broader set of encryption algorithms for best compatibility.		
	<i>high-encryption</i>	Allow only AES-CTR, AES-GCM ciphers and high encryption algorithms.		

## config ssl

Parameter	Description	Type	Size	Default
inspect-all	Level of SSL inspection.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable.		
	<i>certificate-inspection</i>	Inspect SSL handshake only.		
	<i>deep-inspection</i>	Full SSL inspection.		
client-certificate	Action based on received client certificate.	option	-	bypass
	<b>Option</b>	<b>Description</b>		
	<i>bypass</i>	Bypass the session.		
	<i>inspect</i>	Inspect the session.		
	<i>block</i>	Block the session.		
unsupported-ssl-version	Action based on the SSL version used being unsupported.	option	-	block
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Bypass the session when the version is not supported.		
	<i>block</i>	Block the session when the version is not supported.		
unsupported-ssl-cipher	Action based on the SSL cipher used being unsupported.	option	-	allow
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Bypass the session when the cipher is not supported.		
	<i>block</i>	Block the session when the cipher is not supported.		
unsupported-ssl-negotiation	Action based on the SSL negotiation used being unsupported.	option	-	allow

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Bypass the session when the negotiation is not supported.		
	<i>block</i>	Block the session when the negotiation is not supported.		
expired-server-cert	Action based on server certificate is expired.	option	-	block
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow the server certificate.		
	<i>block</i>	Block the session.		
	<i>ignore</i>	Re-sign the server certificate as trusted.		
revoked-server-cert	Action based on server certificate is revoked.	option	-	block
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow the server certificate.		
	<i>block</i>	Block the session.		
	<i>ignore</i>	Re-sign the server certificate as trusted.		
untrusted-server-cert	Action based on server certificate is not issued by a trusted CA.	option	-	allow
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow the server certificate.		
	<i>block</i>	Block the session.		
	<i>ignore</i>	Re-sign the server certificate as trusted.		
cert-validation-timeout	Action based on certificate validation timeout.	option	-	allow
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow the server certificate.		
	<i>block</i>	Block the session.		
	<i>ignore</i>	Re-sign the server certificate as trusted.		
cert-validation-failure	Action based on certificate validation failure.	option	-	block

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow the server certificate.		
	<i>block</i>	Block the session.		
	<i>ignore</i>	Re-sign the server certificate as trusted.		
sni-server-cert-check	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.		
	<i>strict</i>	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.		
	<i>disable</i>	Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.		
cert-probe-failure	Action based on certificate probe failure.	option	-	block
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Bypass the session when unable to retrieve server's certificate for inspection.		
	<i>block</i>	Block the session when unable to retrieve server's certificate for inspection.		
min-allowed-ssl-version	Minimum SSL version to be allowed. Flow-based inspection does not support SSL version control.	option	-	tls-1.1
	<b>Option</b>	<b>Description</b>		
	<i>ssl-3.0</i>	SSL 3.0.		
	<i>tls-1.0</i>	TLS 1.0.		
	<i>tls-1.1</i>	TLS 1.1.		
	<i>tls-1.2</i>	TLS 1.2.		
	<i>tls-1.3</i>	TLS 1.3.		

## config ssl-exempt

Parameter	Description	Type	Size	Default
id	ID number.	integer	Minimum value: 0 Maximum value: 512	0
type	Type of address object (IPv4 or IPv6) or FortiGuard category.	option	-	fortiguard-category
	<b>Option</b>	<b>Description</b>		
	<i>fortiguard-category</i>	FortiGuard category.		
	<i>address</i>	Firewall IPv4 address.		
	<i>address6</i>	Firewall IPv6 address.		
	<i>wildcard-fqdn</i>	Fully Qualified Domain Name with wildcard characters.		
	<i>regex</i>	Regular expression FQDN.		
fortiguard-category	FortiGuard category ID.	integer	Minimum value: 0 Maximum value: 255	0
address	IPv4 address object.	string	Maximum length: 79	
address6	IPv6 address object.	string	Maximum length: 79	
wildcard-fqdn	Exempt servers by wildcard FQDN.	string	Maximum length: 79	
regex	Exempt servers by regular expression.	string	Maximum length: 255	

## config ssl-server

Parameter	Description	Type	Size	Default
id	SSL server ID.	integer	Minimum value: 0 Maximum value: 4294967295	0



Parameter	Description	Type	Size	Default								
ip	IPv4 address of the SSL server.	ipv4-address-any	Not Specified	0.0.0.0								
https-client-certificate	Action based on received client certificate during the HTTPS handshake.	option	-	bypass								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>bypass</td><td>Bypass the session.</td></tr><tr><td>inspect</td><td>Inspect the session.</td></tr><tr><td>block</td><td>Block the session.</td></tr></table>	Option	Description	bypass	Bypass the session.	inspect	Inspect the session.	block	Block the session.			
Option	Description											
bypass	Bypass the session.											
inspect	Inspect the session.											
block	Block the session.											
smtps-client-certificate	Action based on received client certificate during the SMTPS handshake.	option	-	bypass								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>bypass</td><td>Bypass the session.</td></tr><tr><td>inspect</td><td>Inspect the session.</td></tr><tr><td>block</td><td>Block the session.</td></tr></table>	Option	Description	bypass	Bypass the session.	inspect	Inspect the session.	block	Block the session.			
Option	Description											
bypass	Bypass the session.											
inspect	Inspect the session.											
block	Block the session.											
pop3s-client-certificate	Action based on received client certificate during the POP3S handshake.	option	-	bypass								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>bypass</td><td>Bypass the session.</td></tr><tr><td>inspect</td><td>Inspect the session.</td></tr><tr><td>block</td><td>Block the session.</td></tr></table>	Option	Description	bypass	Bypass the session.	inspect	Inspect the session.	block	Block the session.			
Option	Description											
bypass	Bypass the session.											
inspect	Inspect the session.											
block	Block the session.											
imaps-client-certificate	Action based on received client certificate during the IMAPS handshake.	option	-	bypass								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>bypass</td><td>Bypass the session.</td></tr><tr><td>inspect</td><td>Inspect the session.</td></tr><tr><td>block</td><td>Block the session.</td></tr></table>	Option	Description	bypass	Bypass the session.	inspect	Inspect the session.	block	Block the session.			
Option	Description											
bypass	Bypass the session.											
inspect	Inspect the session.											
block	Block the session.											
ftps-client-certificate	Action based on received client certificate during the FTPS handshake.	option	-	bypass								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>bypass</td><td>Bypass the session.</td></tr></table>	Option	Description	bypass	Bypass the session.							
Option	Description											
bypass	Bypass the session.											

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>inspect</i>	Inspect the session.		
	<i>block</i>	Block the session.		
ssl-other-client-certificate	Action based on received client certificate during an SSL protocol handshake.	option	-	bypass
	<b>Option</b>	<b>Description</b>		
	<i>bypass</i>	Bypass the session.		
	<i>inspect</i>	Inspect the session.		
	<i>block</i>	Block the session.		

## config firewall ssl setting

SSL proxy settings.

```
config firewall ssl setting
    Description: SSL proxy settings.
    set abbreviate-handshake [enable|disable]
    set cert-cache-capacity {integer}
    set cert-cache-timeout {integer}
    set kxp-queue-threshold {integer}
    set no-matching-cipher-action [bypass|drop]
    set proxy-connect-timeout {integer}
    set session-cache-capacity {integer}
    set session-cache-timeout {integer}
    set ssl-dh-bits [768|1024|...]
    set ssl-queue-threshold {integer}
    set ssl-send-empty-frags [enable|disable]
end
```

## config firewall ssl setting

Parameter	Description	Type	Size	Default
abbreviate-handshake	Enable/disable use of SSL abbreviated handshake.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable use of SSL abbreviated handshake.		
	<i>disable</i>	Disable use of SSL abbreviated handshake.		

Parameter	Description	Type	Size	Default										
cert-cache-capacity	Maximum capacity of the host certificate cache.	integer	Minimum value: 0 Maximum value: 500	200										
cert-cache-timeout	Time limit to keep certificate cache.	integer	Minimum value: 1 Maximum value: 120	10										
kxp-queue-threshold *	Maximum length of the CP KXP queue. When the queue becomes full, the proxy switches cipher functions to the main CPU.	integer	Minimum value: 0 Maximum value: 512	16										
no-matching-cipher-action	Bypass or drop the connection when no matching cipher is found.	option	-	bypass										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>bypass</td><td>Bypass connection.</td></tr><tr><td>drop</td><td>Drop connection.</td></tr></table>				Option	Description	bypass	Bypass connection.	drop	Drop connection.				
Option	Description													
bypass	Bypass connection.													
drop	Drop connection.													
proxy-connect-timeout	Time limit to make an internal connection to the appropriate proxy process.	integer	Minimum value: 1 Maximum value: 60	30										
session-cache-capacity	Capacity of the SSL session cache.	integer	Minimum value: 0 Maximum value: 1000	500										
session-cache-timeout	Time limit to keep SSL session state.	integer	Minimum value: 1 Maximum value: 60	20										
ssl-dh-bits	Bit-size of Diffie-Hellman.	option	-	2048										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>768</td><td>768-bit Diffie-Hellman prime.</td></tr><tr><td>1024</td><td>1024-bit Diffie-Hellman prime.</td></tr><tr><td>1536</td><td>1536-bit Diffie-Hellman prime.</td></tr><tr><td>2048</td><td>2048-bit Diffie-Hellman prime.</td></tr></table>				Option	Description	768	768-bit Diffie-Hellman prime.	1024	1024-bit Diffie-Hellman prime.	1536	1536-bit Diffie-Hellman prime.	2048	2048-bit Diffie-Hellman prime.
Option	Description													
768	768-bit Diffie-Hellman prime.													
1024	1024-bit Diffie-Hellman prime.													
1536	1536-bit Diffie-Hellman prime.													
2048	2048-bit Diffie-Hellman prime.													

Parameter	Description	Type	Size	Default						
ssl-queue-threshold *	Maximum length of the CP SSL queue. When the queue becomes full, the proxy switches cipher functions to the main CPU.	integer	Minimum value: 0 Maximum value: 512	32						
ssl-send-empty-frags	Enable/disable sending empty fragments to avoid attack on CBC IV (for SSL 3.0 and TLS 1.0 only).	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Send empty fragments.</td></tr><tr><td><i>disable</i></td><td>Do not send empty fragments.</td></tr></table>				Option	Description	<i>enable</i>	Send empty fragments.	<i>disable</i>	Do not send empty fragments.
Option	Description									
<i>enable</i>	Send empty fragments.									
<i>disable</i>	Do not send empty fragments.									

\* This parameter may not exist in some models.

## config firewall traffic-class

Configure names for shaping classes.

```
config firewall traffic-class
    Description: Configure names for shaping classes.
    edit <class-id>
        set class-name {string}
    next
end
```

## config firewall traffic-class

Parameter	Description	Type	Size	Default
class-id	Class ID to be named.	integer	Minimum value: 2 Maximum value: 31	0
class-name	Define the name for this class-id.	string	Maximum length: 35	

## config firewall ttl-policy

Configure TTL policies.

```
config firewall ttl-policy
    Description: Configure TTL policies.
    edit <id>
        set action [accept|deny]
        set schedule {string}
        set service <name1>, <name2>, ...
```

```

        set srcaddr <name1>, <name2>, ...
        set srcintf {string}
        set status [enable|disable]
        set ttl {user}
    next
end

```

## config firewall ttl-policy

Parameter	Description	Type	Size	Default						
action	Action to be performed on traffic matching this policy.	option	-	deny						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>accept</i></td><td>Allow traffic matching this policy.</td></tr><tr><td><i>deny</i></td><td>Deny or block traffic matching this policy.</td></tr></table>				Option	Description	<i>accept</i>	Allow traffic matching this policy.	<i>deny</i>	Deny or block traffic matching this policy.
	Option	Description								
	<i>accept</i>	Allow traffic matching this policy.								
<i>deny</i>	Deny or block traffic matching this policy.									
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0						
schedule	Schedule object from available options.	string	Maximum length: 35							
service <name>	Service object(s) from available options. Separate multiple names with a space. Service name.	string	Maximum length: 79							
srcaddr <name>	Source address object(s) from available options. Separate multiple names with a space. Address name.	string	Maximum length: 79							
srcintf	Source interface name from available interfaces.	string	Maximum length: 35							
status	Enable/disable this TTL policy.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable this TTL policy.</td></tr><tr><td><i>disable</i></td><td>Disable this TTL policy.</td></tr></table>				Option	Description	<i>enable</i>	Enable this TTL policy.	<i>disable</i>	Disable this TTL policy.
	Option	Description								
	<i>enable</i>	Enable this TTL policy.								
<i>disable</i>	Disable this TTL policy.									
ttl	Value/range to match against the packet's Time to Live value.	user	Not Specified							

## config firewall vendor-mac

Show vendor and the MAC address they have.

```

config firewall vendor-mac
    Description: Show vendor and the MAC address they have.
    edit <id>
        set mac-number {integer}
        set name {string}
        set obsolete {integer}
    next
end

```

## config firewall vendor-mac

Parameter	Description	Type	Size	Default
id	Vendor ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
mac-number	Total number of MAC addresses.	integer	Minimum value: 0 Maximum value: 4294967295	0
name	Vendor name.	string	Maximum length: 63	
obsolete	Indicates whether the Vendor ID can be used.	integer	Minimum value: 0 Maximum value: 255	0

## config firewall vip

Configure virtual IP for IPv4.

```

config firewall vip
    Description: Configure virtual IP for IPv4.
    edit <name>
        set add-nat46-route [disable|enable]
        set arp-reply [disable|enable]
        set color {integer}
        set comment {var-string}
        set dns-mapping-ttl {integer}
        set extaddr <name1>, <name2>, ...
        set extintf {string}
        set extip {user}
        set extport {user}
        set gratuitous-arp-interval {integer}
        set http-cookie-age {integer}
        set http-cookie-domain {string}
        set http-cookie-domain-from-host [disable|enable]
    end
end

```

```

set http-cookie-generation {integer}
set http-cookie-path {string}
set http-cookie-share [disable|same-ip]
set http-ip-header [enable|disable]
set http-ip-header-name {string}
set http-multiplex [enable|disable]
set http-redirect [enable|disable]
set https-cookie-secure [disable|enable]
set id {integer}
set ipv6-mappedip {user}
set ipv6-mappedport {user}
set ldb-method [static|round-robin|...]
set mapped-addr {string}
set mappedip <range1>, <range2>, ...
set mappedport {user}
set max-embryonic-connections {integer}
set monitor <name1>, <name2>, ...
set nat-source-vip [disable|enable]
set nat44 [disable|enable]
set nat46 [disable|enable]
set outlook-web-access [disable|enable]
set persistence [none|http-cookie|...]
set portforward [disable|enable]
set portmapping-type [1-to-1|m-to-n]
set protocol [tcp|udp|...]
config realservers

```

Description: Select the real servers that this server load balancing VIP will distribute traffic to.

```

edit <id>
    set type [ip|address]
    set address {string}
    set ip {user}
    set port {integer}
    set status [active|standby|...]
    set weight {integer}
    set holddown-interval {integer}
    set healthcheck [disable|enable|...]
    set http-host {string}
    set max-connections {integer}
    set monitor <name1>, <name2>, ...
    set client-ip {user}
next
end
set server-type [http|https|...]
set service <name1>, <name2>, ...
set src-filter <range1>, <range2>, ...
set srcintf-filter <interface-name1>, <interface-name2>, ...
set ssl-accept-ffdhe-groups [enable|disable]
set ssl-algorithm [high|medium|...]
set ssl-certificate {string}
config ssl-cipher-suites

```

Description: SSL/TLS cipher suites acceptable from a client, ordered by priority.

```

edit <priority>
    set cipher [TLS-AES-128-GCM-SHA256|TLS-AES-256-GCM-SHA384|...]
    set versions {option1}, {option2}, ...

```

```

        next
    end
    set ssl-client-fallback [disable|enable]
    set ssl-client-rekey-count {integer}
    set ssl-client-renegotiation [allow|deny|...]
    set ssl-client-session-state-max {integer}
    set ssl-client-session-state-timeout {integer}
    set ssl-client-session-state-type [disable|time|...]
    set ssl-dh-bits [768|1024|...]
    set ssl-hpkip [disable|enable|...]
    set ssl-hpkip-age {integer}
    set ssl-hpkip-backup {string}
    set ssl-hpkip-include-subdomains [disable|enable]
    set ssl-hpkip-primary {string}
    set ssl-hpkip-report-uri {var-string}
    set ssl-hsts [disable|enable]
    set ssl-hsts-age {integer}
    set ssl-hsts-include-subdomains [disable|enable]
    set ssl-http-location-conversion [enable|disable]
    set ssl-http-match-host [enable|disable]
    set ssl-max-version [ssl-3.0|tls-1.0|...]
    set ssl-min-version [ssl-3.0|tls-1.0|...]
    set ssl-mode [half|full]
    set ssl-pfs [require|deny|...]
    set ssl-send-empty-frags [enable|disable]
    set ssl-server-algorithm [high|medium|...]
    config ssl-server-cipher-suites
        Description: SSL/TLS cipher suites to offer to a server, ordered by priority.
        edit <priority>
            set cipher [TLS-AES-128-GCM-SHA256|TLS-AES-256-GCM-SHA384|...]
            set versions {option1}, {option2}, ...
        next
    end
    set ssl-server-max-version [ssl-3.0|tls-1.0|...]
    set ssl-server-min-version [ssl-3.0|tls-1.0|...]
    set ssl-server-session-state-max {integer}
    set ssl-server-session-state-timeout {integer}
    set ssl-server-session-state-type [disable|time|...]
    set status [disable|enable]
    set type [static-nat|load-balance|...]
    set uuid {uuid}
    set weblogic-server [disable|enable]
    set websphere-server [disable|enable]
next
end

```

## config firewall vip

Parameter	Description	Type	Size	Default
add-nat46-route	Enable/disable adding NAT46 route.	option	-	enable



Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable adding NAT46 route.</td></tr><tr><td><i>enable</i></td><td>Enable adding NAT46 route.</td></tr></table>	Option	Description	<i>disable</i>	Disable adding NAT46 route.	<i>enable</i>	Enable adding NAT46 route.			
	Option	Description								
	<i>disable</i>	Disable adding NAT46 route.								
<i>enable</i>	Enable adding NAT46 route.									
arp-reply	Enable to respond to ARP requests for this virtual IP address. Enabled by default.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable ARP reply.</td></tr><tr><td><i>enable</i></td><td>Enable ARP reply.</td></tr></table>	Option	Description	<i>disable</i>	Disable ARP reply.	<i>enable</i>	Enable ARP reply.			
	Option	Description								
	<i>disable</i>	Disable ARP reply.								
<i>enable</i>	Enable ARP reply.									
color	Color of icon on the GUI.	integer	Minimum value: 0 Maximum value: 32	0						
comment	Comment.	var-string	Maximum length: 255							
dns-mapping-ttl	DNS mapping TTL.	integer	Minimum value: 0 Maximum value: 604800	0						
extaddr <name>	External FQDN address name. Address name.	string	Maximum length: 79							
extintf	Interface connected to the source network that receives the packets that will be forwarded to the destination network.	string	Maximum length: 35							
extip	IP address or address range on the external interface that you want to map to an address or address range on the destination network.	user	Not Specified							
extport	Incoming port number range that you want to map to a port number range on the destination network.	user	Not Specified							
gratuitous-arp-interval	Enable to have the VIP send gratuitous ARPs. 0=disabled. Set from 5 up to 8640000 seconds to enable.	integer	Minimum value: 5 Maximum value: 8640000	0						

Parameter	Description	Type	Size	Default						
http-cookie-age	Time in minutes that client web browsers should keep a cookie. Default is 60 minutes. 0 = no time limit.	integer	Minimum value: 0 Maximum value: 525600	60						
http-cookie-domain	Domain that HTTP cookie persistence should apply to.	string	Maximum length: 35							
http-cookie-domain-from-host	Enable/disable use of HTTP cookie domain from host field in HTTP.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable use of HTTP cookie domain from host field in HTTP (use http-cooke-domain setting).</td></tr><tr><td><i>enable</i></td><td>Enable use of HTTP cookie domain from host field in HTTP.</td></tr></table>				Option	Description	<i>disable</i>	Disable use of HTTP cookie domain from host field in HTTP (use http-cooke-domain setting).	<i>enable</i>	Enable use of HTTP cookie domain from host field in HTTP.
Option	Description									
<i>disable</i>	Disable use of HTTP cookie domain from host field in HTTP (use http-cooke-domain setting).									
<i>enable</i>	Enable use of HTTP cookie domain from host field in HTTP.									
http-cookie-generation	Generation of HTTP cookie to be accepted. Changing invalidates all existing cookies.	integer	Minimum value: 0 Maximum value: 4294967295	0						
http-cookie-path	Limit HTTP cookie persistence to the specified path.	string	Maximum length: 35							
http-cookie-share	Control sharing of cookies across virtual servers. Use of same-ip means a cookie from one virtual server can be used by another. Disable stops cookie sharing.	option	-	same-ip						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Only allow HTTP cookie to match this virtual server.</td></tr><tr><td><i>same-ip</i></td><td>Allow HTTP cookie to match any virtual server with same IP.</td></tr></table>				Option	Description	<i>disable</i>	Only allow HTTP cookie to match this virtual server.	<i>same-ip</i>	Allow HTTP cookie to match any virtual server with same IP.
Option	Description									
<i>disable</i>	Only allow HTTP cookie to match this virtual server.									
<i>same-ip</i>	Allow HTTP cookie to match any virtual server with same IP.									
http-ip-header	For HTTP multiplexing, enable to add the original client IP address in the XForwarded-For HTTP header.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable adding HTTP header.</td></tr><tr><td><i>disable</i></td><td>Disable adding HTTP header.</td></tr></table>				Option	Description	<i>enable</i>	Enable adding HTTP header.	<i>disable</i>	Disable adding HTTP header.
Option	Description									
<i>enable</i>	Enable adding HTTP header.									
<i>disable</i>	Disable adding HTTP header.									

Parameter	Description	Type	Size	Default						
http-ip-header-name	For HTTP multiplexing, enter a custom HTTPS header name. The original client IP address is added to this header. If empty, X-Forwarded-For is used.	string	Maximum length: 35							
http-multiplex	Enable/disable HTTP multiplexing.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable HTTP session multiplexing.</td></tr><tr><td><i>disable</i></td><td>Disable HTTP session multiplexing.</td></tr></table>	Option	Description	<i>enable</i>	Enable HTTP session multiplexing.	<i>disable</i>	Disable HTTP session multiplexing.			
Option	Description									
<i>enable</i>	Enable HTTP session multiplexing.									
<i>disable</i>	Disable HTTP session multiplexing.									
http-redirect	Enable/disable redirection of HTTP to HTTPS.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable redirection of HTTP to HTTPS.</td></tr><tr><td><i>disable</i></td><td>Disable redirection of HTTP to HTTPS.</td></tr></table>	Option	Description	<i>enable</i>	Enable redirection of HTTP to HTTPS.	<i>disable</i>	Disable redirection of HTTP to HTTPS.			
Option	Description									
<i>enable</i>	Enable redirection of HTTP to HTTPS.									
<i>disable</i>	Disable redirection of HTTP to HTTPS.									
https-cookie-secure	Enable/disable verification that inserted HTTPS cookies are secure.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Do not mark cookie as secure, allow sharing between an HTTP and HTTPS connection.</td></tr><tr><td><i>enable</i></td><td>Mark inserted cookie as secure, cookie can only be used for HTTPS a connection.</td></tr></table>	Option	Description	<i>disable</i>	Do not mark cookie as secure, allow sharing between an HTTP and HTTPS connection.	<i>enable</i>	Mark inserted cookie as secure, cookie can only be used for HTTPS a connection.			
Option	Description									
<i>disable</i>	Do not mark cookie as secure, allow sharing between an HTTP and HTTPS connection.									
<i>enable</i>	Mark inserted cookie as secure, cookie can only be used for HTTPS a connection.									
id	Custom defined ID.	integer	Minimum value: 0 Maximum value: 65535	0						
ipv6-mappedip	Range of mapped IPv6 addresses. Specify the start IPv6 address followed by a space and the end IPv6 address.	user	Not Specified							
ipv6-mappedport	IPv6 port number range on the destination network to which the external port number range is mapped.	user	Not Specified							
ldb-method	Method used to distribute sessions to real servers.	option	-	static						

Parameter	Description	Type	Size	Default																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>static</i></td><td>Distribute to server based on source IP.</td></tr><tr><td><i>round-robin</i></td><td>Distribute to server based round robin order.</td></tr><tr><td><i>weighted</i></td><td>Distribute to server based on weight.</td></tr><tr><td><i>least-session</i></td><td>Distribute to server with lowest session count.</td></tr><tr><td><i>least-rtt</i></td><td>Distribute to server with lowest Round-Trip-Time.</td></tr><tr><td><i>first-alive</i></td><td>Distribute to the first server that is alive.</td></tr><tr><td><i>http-host</i></td><td>Distribute to server based on host field in HTTP header.</td></tr></table>	Option	Description	<i>static</i>	Distribute to server based on source IP.	<i>round-robin</i>	Distribute to server based round robin order.	<i>weighted</i>	Distribute to server based on weight.	<i>least-session</i>	Distribute to server with lowest session count.	<i>least-rtt</i>	Distribute to server with lowest Round-Trip-Time.	<i>first-alive</i>	Distribute to the first server that is alive.	<i>http-host</i>	Distribute to server based on host field in HTTP header.			
	Option	Description																		
	<i>static</i>	Distribute to server based on source IP.																		
	<i>round-robin</i>	Distribute to server based round robin order.																		
	<i>weighted</i>	Distribute to server based on weight.																		
	<i>least-session</i>	Distribute to server with lowest session count.																		
	<i>least-rtt</i>	Distribute to server with lowest Round-Trip-Time.																		
	<i>first-alive</i>	Distribute to the first server that is alive.																		
<i>http-host</i>	Distribute to server based on host field in HTTP header.																			
mapped-addr	Mapped FQDN address name.	string	Maximum length: 79																	
mappedip <range>	IP address or address range on the destination network to which the external IP address is mapped. Mapped IP range.	string	Maximum length: 79																	
mappedport	Port number range on the destination network to which the external port number range is mapped.	user	Not Specified																	
max-embryonic-connections	Maximum number of incomplete connections.	integer	Minimum value: 0 Maximum value: 100000	1000																
monitor <name>	Name of the health check monitor to use when polling to determine a virtual server's connectivity status. Health monitor name.	string	Maximum length: 79																	
name	Virtual IP name.	string	Maximum length: 79																	
nat-source-vip	Enable/disable forcing the source NAT mapped IP to the external IP for all traffic.	option	-	disable																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Force only the source NAT mapped IP to the external IP for traffic egressing the external interface of the VIP.</td></tr><tr><td><i>enable</i></td><td>Force the source NAT mapped IP to the external IP for all traffic.</td></tr></table>	Option	Description	<i>disable</i>	Force only the source NAT mapped IP to the external IP for traffic egressing the external interface of the VIP.	<i>enable</i>	Force the source NAT mapped IP to the external IP for all traffic.													
	Option	Description																		
	<i>disable</i>	Force only the source NAT mapped IP to the external IP for traffic egressing the external interface of the VIP.																		
<i>enable</i>	Force the source NAT mapped IP to the external IP for all traffic.																			
nat44	Enable/disable NAT44.	option	-	enable																

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable NAT44.		
	<i>enable</i>	Enable NAT44.		
nat46	Enable/disable NAT46.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable NAT46.		
	<i>enable</i>	Enable NAT46.		
outlook-web-access	Enable to add the Front-End-Https header for Microsoft Outlook Web Access.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable Outlook Web Access support.		
	<i>enable</i>	Enable Outlook Web Access support.		
persistence	Configure how to make sure that clients connect to the same server every time they make a request that is part of the same session.	option	-	none
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	None.		
	<i>http-cookie</i>	HTTP cookie.		
	<i>ssl-session-id</i>	SSL session ID.		
portforward	Enable/disable port forwarding.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable port forward.		
	<i>enable</i>	Enable port forward.		
portmapping-type	Port mapping type.	option	-	1-to-1
	<b>Option</b>	<b>Description</b>		
	<i>1-to-1</i>	One to one.		
	<i>m-to-n</i>	Many to many.		

Parameter	Description	Type	Size	Default																				
protocol	Protocol to use when forwarding packets.	option	-	tcp																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>tcp</td><td>TCP.</td></tr><tr><td>udp</td><td>UDP.</td></tr><tr><td>sctp</td><td>SCTP.</td></tr><tr><td>icmp</td><td>ICMP.</td></tr></table>	Option	Description	tcp	TCP.	udp	UDP.	sctp	SCTP.	icmp	ICMP.													
	Option	Description																						
	tcp	TCP.																						
	udp	UDP.																						
	sctp	SCTP.																						
icmp	ICMP.																							
server-type	Protocol to be load balanced by the virtual server (also called the server load balance virtual IP).	option	-																					
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>http</td><td>HTTP.</td></tr><tr><td>https</td><td>HTTPS.</td></tr><tr><td>imaps</td><td>IMAPS.</td></tr><tr><td>pop3s</td><td>POP3S.</td></tr><tr><td>smtps</td><td>SMTPS.</td></tr><tr><td>ssl</td><td>SSL.</td></tr><tr><td>tcp</td><td>TCP.</td></tr><tr><td>udp</td><td>UDP.</td></tr><tr><td>ip</td><td>IP.</td></tr></table>	Option	Description	http	HTTP.	https	HTTPS.	imaps	IMAPS.	pop3s	POP3S.	smtps	SMTPS.	ssl	SSL.	tcp	TCP.	udp	UDP.	ip	IP.			
	Option	Description																						
	http	HTTP.																						
	https	HTTPS.																						
	imaps	IMAPS.																						
	pop3s	POP3S.																						
	smtps	SMTPS.																						
	ssl	SSL.																						
	tcp	TCP.																						
	udp	UDP.																						
ip	IP.																							
service <name>	Service name. Service name.	string	Maximum length: 79																					
src-filter <range>	Source address filter. Each address must be either an IP/subnet (x.x.x.x/n) or a range (x.x.x.x-y.y.y.y). Separate addresses with spaces. Source-filter range.	string	Maximum length: 79																					
srcintf-filter <interface-name>	Interfaces to which the VIP applies. Separate the names with spaces. Interface name.	string	Maximum length: 79																					
ssl-accept-ffdhe-groups	Enable/disable FFDHE cipher suite for SSL key exchange.	option	-	enable																				

Parameter	Description	Type	Size	Default										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Accept FFDHE groups.</td></tr><tr><td><i>disable</i></td><td>Do not accept FFDHE groups.</td></tr></table>	Option	Description	<i>enable</i>	Accept FFDHE groups.	<i>disable</i>	Do not accept FFDHE groups.							
	Option	Description												
	<i>enable</i>	Accept FFDHE groups.												
<i>disable</i>	Do not accept FFDHE groups.													
ssl-algorithm	Permitted encryption algorithms for SSL sessions according to encryption strength.	option	-	high										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>high</i></td><td>High encryption. Allow only AES and ChaCha.</td></tr><tr><td><i>medium</i></td><td>Medium encryption. Allow AES, ChaCha, 3DES, and RC4.</td></tr><tr><td><i>low</i></td><td>Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.</td></tr><tr><td><i>custom</i></td><td>Custom encryption. Use config ssl-cipher-suites to select the cipher suites that are allowed.</td></tr></table>	Option	Description	<i>high</i>	High encryption. Allow only AES and ChaCha.	<i>medium</i>	Medium encryption. Allow AES, ChaCha, 3DES, and RC4.	<i>low</i>	Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.	<i>custom</i>	Custom encryption. Use config ssl-cipher-suites to select the cipher suites that are allowed.			
	Option	Description												
	<i>high</i>	High encryption. Allow only AES and ChaCha.												
	<i>medium</i>	Medium encryption. Allow AES, ChaCha, 3DES, and RC4.												
	<i>low</i>	Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.												
<i>custom</i>	Custom encryption. Use config ssl-cipher-suites to select the cipher suites that are allowed.													
ssl-certificate	The name of the certificate to use for SSL handshake.	string	Maximum length: 35											
ssl-client-fallback	Enable/disable support for preventing Downgrade Attacks on client connections (RFC 7507).	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable.</td></tr><tr><td><i>enable</i></td><td>Enable.</td></tr></table>	Option	Description	<i>disable</i>	Disable.	<i>enable</i>	Enable.							
	Option	Description												
	<i>disable</i>	Disable.												
<i>enable</i>	Enable.													
ssl-client-rekey-count	Maximum length of data in MB before triggering a client rekey (0 = disable).	integer	Minimum value: 200 Maximum value: 1048576	0										
ssl-client-renegotiation	Allow, deny, or require secure renegotiation of client sessions to comply with RFC 5746.	option	-	secure										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow a SSL client to renegotiate.</td></tr><tr><td><i>deny</i></td><td>Abort any client initiated SSL re-negotiation attempt.</td></tr><tr><td><i>secure</i></td><td>Abort any client initiated SSL re-negotiation attempt that does not use RFC 5746 Secure Renegotiation.</td></tr></table>	Option	Description	<i>allow</i>	Allow a SSL client to renegotiate.	<i>deny</i>	Abort any client initiated SSL re-negotiation attempt.	<i>secure</i>	Abort any client initiated SSL re-negotiation attempt that does not use RFC 5746 Secure Renegotiation.					
	Option	Description												
	<i>allow</i>	Allow a SSL client to renegotiate.												
	<i>deny</i>	Abort any client initiated SSL re-negotiation attempt.												
<i>secure</i>	Abort any client initiated SSL re-negotiation attempt that does not use RFC 5746 Secure Renegotiation.													

Parameter	Description	Type	Size	Default														
ssl-client-session-state-max	Maximum number of client to FortiGate SSL session states to keep.	integer	Minimum value: 1 Maximum value: 10000	1000														
ssl-client-session-state-timeout	Number of minutes to keep client to FortiGate SSL session state.	integer	Minimum value: 1 Maximum value: 14400	30														
ssl-client-session-state-type	How to expire SSL sessions for the segment of the SSL connection between the client and the FortiGate.	option	-	both														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Do not keep session states.</td></tr><tr><td>time</td><td>Expire session states after this many minutes.</td></tr><tr><td>count</td><td>Expire session states when this maximum is reached.</td></tr><tr><td>both</td><td>Expire session states based on time or count, whichever occurs first.</td></tr></table>	Option	Description	disable	Do not keep session states.	time	Expire session states after this many minutes.	count	Expire session states when this maximum is reached.	both	Expire session states based on time or count, whichever occurs first.							
Option	Description																	
disable	Do not keep session states.																	
time	Expire session states after this many minutes.																	
count	Expire session states when this maximum is reached.																	
both	Expire session states based on time or count, whichever occurs first.																	
ssl-dh-bits	Number of bits to use in the Diffie-Hellman exchange for RSA encryption of SSL sessions.	option	-	2048														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>768</td><td>768-bit Diffie-Hellman prime.</td></tr><tr><td>1024</td><td>1024-bit Diffie-Hellman prime.</td></tr><tr><td>1536</td><td>1536-bit Diffie-Hellman prime.</td></tr><tr><td>2048</td><td>2048-bit Diffie-Hellman prime.</td></tr><tr><td>3072</td><td>3072-bit Diffie-Hellman prime.</td></tr><tr><td>4096</td><td>4096-bit Diffie-Hellman prime.</td></tr></table>	Option	Description	768	768-bit Diffie-Hellman prime.	1024	1024-bit Diffie-Hellman prime.	1536	1536-bit Diffie-Hellman prime.	2048	2048-bit Diffie-Hellman prime.	3072	3072-bit Diffie-Hellman prime.	4096	4096-bit Diffie-Hellman prime.			
Option	Description																	
768	768-bit Diffie-Hellman prime.																	
1024	1024-bit Diffie-Hellman prime.																	
1536	1536-bit Diffie-Hellman prime.																	
2048	2048-bit Diffie-Hellman prime.																	
3072	3072-bit Diffie-Hellman prime.																	
4096	4096-bit Diffie-Hellman prime.																	
ssl-hpkip	Enable/disable including HPKP header in response.	option	-	disable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Do not add a HPKP header to each HTTP response.</td></tr><tr><td>enable</td><td>Add a HPKP header to each a HTTP response.</td></tr><tr><td>report-only</td><td>Add a HPKP Report-Only header to each HTTP response.</td></tr></table>	Option	Description	disable	Do not add a HPKP header to each HTTP response.	enable	Add a HPKP header to each a HTTP response.	report-only	Add a HPKP Report-Only header to each HTTP response.									
Option	Description																	
disable	Do not add a HPKP header to each HTTP response.																	
enable	Add a HPKP header to each a HTTP response.																	
report-only	Add a HPKP Report-Only header to each HTTP response.																	



Parameter	Description	Type	Size	Default						
ssl-hpkp-age	Number of seconds the client should honor the HPKP setting.	integer	Minimum value: 60 Maximum value: 157680000	5184000						
ssl-hpkp-backup	Certificate to generate backup HPKP pin from.	string	Maximum length: 79							
ssl-hpkp-include-subdomains	Indicate that HPKP header applies to all subdomains.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>HPKP header does not apply to subdomains.</td></tr><tr><td>enable</td><td>HPKP header applies to subdomains.</td></tr></table>				Option	Description	disable	HPKP header does not apply to subdomains.	enable	HPKP header applies to subdomains.
	Option	Description								
	disable	HPKP header does not apply to subdomains.								
enable	HPKP header applies to subdomains.									
ssl-hpkp-primary	Certificate to generate primary HPKP pin from.	string	Maximum length: 79							
ssl-hpkp-report-uri	URL to report HPKP violations to.	var-string	Maximum length: 255							
ssl-hsts	Enable/disable including HSTS header in response.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Do not add a HSTS header to each a HTTP response.</td></tr><tr><td>enable</td><td>Add a HSTS header to each HTTP response.</td></tr></table>				Option	Description	disable	Do not add a HSTS header to each a HTTP response.	enable	Add a HSTS header to each HTTP response.
	Option	Description								
	disable	Do not add a HSTS header to each a HTTP response.								
enable	Add a HSTS header to each HTTP response.									
ssl-hsts-age	Number of seconds the client should honor the HSTS setting.	integer	Minimum value: 60 Maximum value: 157680000	5184000						
ssl-hsts-include-subdomains	Indicate that HSTS header applies to all subdomains.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>HSTS header does not apply to subdomains.</td></tr><tr><td>enable</td><td>HSTS header applies to subdomains.</td></tr></table>				Option	Description	disable	HSTS header does not apply to subdomains.	enable	HSTS header applies to subdomains.
	Option	Description								
	disable	HSTS header does not apply to subdomains.								
enable	HSTS header applies to subdomains.									
ssl-http-location-conversion	Enable to replace HTTP with HTTPS in the reply's Location HTTP header field.	option	-	disable						

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable HTTP location conversion.		
	<i>disable</i>	Disable HTTP location conversion.		
ssl-http-match-host	Enable/disable HTTP host matching for location conversion.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Match HTTP host in response header.		
	<i>disable</i>	Do not match HTTP host.		
ssl-max-version	Highest SSL/TLS version acceptable from a client.	option	-	tls-1.3
	<b>Option</b>	<b>Description</b>		
	<i>ssl-3.0</i>	SSL 3.0.		
	<i>tls-1.0</i>	TLS 1.0.		
	<i>tls-1.1</i>	TLS 1.1.		
	<i>tls-1.2</i>	TLS 1.2.		
	<i>tls-1.3</i>	TLS 1.3.		
ssl-min-version	Lowest SSL/TLS version acceptable from a client.	option	-	tls-1.1
	<b>Option</b>	<b>Description</b>		
	<i>ssl-3.0</i>	SSL 3.0.		
	<i>tls-1.0</i>	TLS 1.0.		
	<i>tls-1.1</i>	TLS 1.1.		
	<i>tls-1.2</i>	TLS 1.2.		
	<i>tls-1.3</i>	TLS 1.3.		
ssl-mode	Apply SSL offloading between the client and the FortiGate (half) or from the client to the FortiGate and from the FortiGate to the server (full).	option	-	half
	<b>Option</b>	<b>Description</b>		
	<i>half</i>	Client to FortiGate SSL.		
	<i>full</i>	Client to FortiGate and FortiGate to Server SSL.		

Parameter	Description	Type	Size	Default												
ssl-pfs	Select the cipher suites that can be used for SSL perfect forward secrecy (PFS). Applies to both client and server sessions.	option	-	require												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>require</i></td><td>Allow only Diffie-Hellman cipher-suites, so PFS is applied.</td></tr><tr><td><i>deny</i></td><td>Allow only non-Diffie-Hellman cipher-suites, so PFS is not applied.</td></tr><tr><td><i>allow</i></td><td>Allow use of any cipher suite so PFS may or may not be used depending on the cipher suite selected.</td></tr></table>	Option	Description	<i>require</i>	Allow only Diffie-Hellman cipher-suites, so PFS is applied.	<i>deny</i>	Allow only non-Diffie-Hellman cipher-suites, so PFS is not applied.	<i>allow</i>	Allow use of any cipher suite so PFS may or may not be used depending on the cipher suite selected.							
Option	Description															
<i>require</i>	Allow only Diffie-Hellman cipher-suites, so PFS is applied.															
<i>deny</i>	Allow only non-Diffie-Hellman cipher-suites, so PFS is not applied.															
<i>allow</i>	Allow use of any cipher suite so PFS may or may not be used depending on the cipher suite selected.															
ssl-send-empty-frags	Enable/disable sending empty fragments to avoid CBC IV attacks (SSL 3.0 & TLS 1.0 only). May need to be disabled for compatibility with older systems.	option	-	enable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Send empty fragments.</td></tr><tr><td><i>disable</i></td><td>Do not send empty fragments.</td></tr></table>	Option	Description	<i>enable</i>	Send empty fragments.	<i>disable</i>	Do not send empty fragments.									
Option	Description															
<i>enable</i>	Send empty fragments.															
<i>disable</i>	Do not send empty fragments.															
ssl-server-algorithm	Permitted encryption algorithms for the server side of SSL full mode sessions according to encryption strength.	option	-	client												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>high</i></td><td>High encryption. Allow only AES and ChaCha.</td></tr><tr><td><i>medium</i></td><td>Medium encryption. Allow AES, ChaCha, 3DES, and RC4.</td></tr><tr><td><i>low</i></td><td>Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.</td></tr><tr><td><i>custom</i></td><td>Custom encryption. Use ssl-server-cipher-suites to select the cipher suites that are allowed.</td></tr><tr><td><i>client</i></td><td>Use the same encryption algorithms for both client and server sessions.</td></tr></table>	Option	Description	<i>high</i>	High encryption. Allow only AES and ChaCha.	<i>medium</i>	Medium encryption. Allow AES, ChaCha, 3DES, and RC4.	<i>low</i>	Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.	<i>custom</i>	Custom encryption. Use ssl-server-cipher-suites to select the cipher suites that are allowed.	<i>client</i>	Use the same encryption algorithms for both client and server sessions.			
Option	Description															
<i>high</i>	High encryption. Allow only AES and ChaCha.															
<i>medium</i>	Medium encryption. Allow AES, ChaCha, 3DES, and RC4.															
<i>low</i>	Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.															
<i>custom</i>	Custom encryption. Use ssl-server-cipher-suites to select the cipher suites that are allowed.															
<i>client</i>	Use the same encryption algorithms for both client and server sessions.															
ssl-server-max-version	Highest SSL/TLS version acceptable from a server. Use the client setting by default.	option	-	client												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ssl-3.0</i></td><td>SSL 3.0.</td></tr><tr><td><i>tls-1.0</i></td><td>TLS 1.0.</td></tr><tr><td><i>tls-1.1</i></td><td>TLS 1.1.</td></tr><tr><td><i>tls-1.2</i></td><td>TLS 1.2.</td></tr></table>	Option	Description	<i>ssl-3.0</i>	SSL 3.0.	<i>tls-1.0</i>	TLS 1.0.	<i>tls-1.1</i>	TLS 1.1.	<i>tls-1.2</i>	TLS 1.2.					
Option	Description															
<i>ssl-3.0</i>	SSL 3.0.															
<i>tls-1.0</i>	TLS 1.0.															
<i>tls-1.1</i>	TLS 1.1.															
<i>tls-1.2</i>	TLS 1.2.															

Parameter	Description	Type	Size	Default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>tls-1.3</i></td><td>TLS 1.3.</td></tr><tr><td><i>client</i></td><td>Use same value as client configuration.</td></tr></table>	Option	Description	<i>tls-1.3</i>	TLS 1.3.	<i>client</i>	Use same value as client configuration.											
	Option	Description																
	<i>tls-1.3</i>	TLS 1.3.																
<i>client</i>	Use same value as client configuration.																	
ssl-server-min-version	Lowest SSL/TLS version acceptable from a server. Use the client setting by default.	option	-	client														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ssl-3.0</i></td><td>SSL 3.0.</td></tr><tr><td><i>tls-1.0</i></td><td>TLS 1.0.</td></tr><tr><td><i>tls-1.1</i></td><td>TLS 1.1.</td></tr><tr><td><i>tls-1.2</i></td><td>TLS 1.2.</td></tr><tr><td><i>tls-1.3</i></td><td>TLS 1.3.</td></tr><tr><td><i>client</i></td><td>Use same value as client configuration.</td></tr></table>	Option	Description	<i>ssl-3.0</i>	SSL 3.0.	<i>tls-1.0</i>	TLS 1.0.	<i>tls-1.1</i>	TLS 1.1.	<i>tls-1.2</i>	TLS 1.2.	<i>tls-1.3</i>	TLS 1.3.	<i>client</i>	Use same value as client configuration.			
	Option	Description																
	<i>ssl-3.0</i>	SSL 3.0.																
	<i>tls-1.0</i>	TLS 1.0.																
	<i>tls-1.1</i>	TLS 1.1.																
	<i>tls-1.2</i>	TLS 1.2.																
	<i>tls-1.3</i>	TLS 1.3.																
<i>client</i>	Use same value as client configuration.																	
ssl-server-session-state-max	Maximum number of FortiGate to Server SSL session states to keep.	integer	Minimum value: 1 Maximum value: 10000	100														
ssl-server-session-state-timeout	Number of minutes to keep FortiGate to Server SSL session state.	integer	Minimum value: 1 Maximum value: 14400	60														
ssl-server-session-state-type	How to expire SSL sessions for the segment of the SSL connection between the server and the FortiGate.	option	-	both														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Do not keep session states.</td></tr><tr><td><i>time</i></td><td>Expire session states after this many minutes.</td></tr><tr><td><i>count</i></td><td>Expire session states when this maximum is reached.</td></tr><tr><td><i>both</i></td><td>Expire session states based on time or count, whichever occurs first.</td></tr></table>	Option	Description	<i>disable</i>	Do not keep session states.	<i>time</i>	Expire session states after this many minutes.	<i>count</i>	Expire session states when this maximum is reached.	<i>both</i>	Expire session states based on time or count, whichever occurs first.							
	Option	Description																
	<i>disable</i>	Do not keep session states.																
	<i>time</i>	Expire session states after this many minutes.																
<i>count</i>	Expire session states when this maximum is reached.																	
<i>both</i>	Expire session states based on time or count, whichever occurs first.																	
status	Enable/disable VIP.	option	-	enable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable the VIP.</td></tr><tr><td><i>enable</i></td><td>Enable the VIP.</td></tr></table>	Option	Description	<i>disable</i>	Disable the VIP.	<i>enable</i>	Enable the VIP.											
	Option	Description																
	<i>disable</i>	Disable the VIP.																
<i>enable</i>	Enable the VIP.																	

Parameter	Description	Type	Size	Default														
type	Configure a static NAT, load balance, server load balance, access proxy, DNS translation, or FQDN VIP.	option	-	static-nat														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>static-nat</i></td><td>Static NAT.</td></tr><tr><td><i>load-balance</i></td><td>Load balance.</td></tr><tr><td><i>server-load-balance</i></td><td>Server load balance.</td></tr><tr><td><i>dns-translation</i></td><td>DNS translation.</td></tr><tr><td><i>fqdn</i></td><td>Fully qualified domain name.</td></tr><tr><td><i>access-proxy</i></td><td>Access proxy.</td></tr></table>	Option	Description	<i>static-nat</i>	Static NAT.	<i>load-balance</i>	Load balance.	<i>server-load-balance</i>	Server load balance.	<i>dns-translation</i>	DNS translation.	<i>fqdn</i>	Fully qualified domain name.	<i>access-proxy</i>	Access proxy.			
Option	Description																	
<i>static-nat</i>	Static NAT.																	
<i>load-balance</i>	Load balance.																	
<i>server-load-balance</i>	Server load balance.																	
<i>dns-translation</i>	DNS translation.																	
<i>fqdn</i>	Fully qualified domain name.																	
<i>access-proxy</i>	Access proxy.																	
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000														
weblogic-server	Enable to add an HTTP header to indicate SSL offloading for a WebLogic server.	option	-	disable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Do not add HTTP header indicating SSL offload for WebLogic server.</td></tr><tr><td><i>enable</i></td><td>Add HTTP header indicating SSL offload for WebLogic server.</td></tr></table>	Option	Description	<i>disable</i>	Do not add HTTP header indicating SSL offload for WebLogic server.	<i>enable</i>	Add HTTP header indicating SSL offload for WebLogic server.											
Option	Description																	
<i>disable</i>	Do not add HTTP header indicating SSL offload for WebLogic server.																	
<i>enable</i>	Add HTTP header indicating SSL offload for WebLogic server.																	
websphere-server	Enable to add an HTTP header to indicate SSL offloading for a WebSphere server.	option	-	disable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Do not add HTTP header indicating SSL offload for WebSphere server.</td></tr><tr><td><i>enable</i></td><td>Add HTTP header indicating SSL offload for WebSphere server.</td></tr></table>	Option	Description	<i>disable</i>	Do not add HTTP header indicating SSL offload for WebSphere server.	<i>enable</i>	Add HTTP header indicating SSL offload for WebSphere server.											
Option	Description																	
<i>disable</i>	Do not add HTTP header indicating SSL offload for WebSphere server.																	
<i>enable</i>	Add HTTP header indicating SSL offload for WebSphere server.																	

## config realservers

Parameter	Description	Type	Size	Default
id	Real server ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
type	Type of address.	option	-	ip

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ip</i></td><td>Standard IPv4 address.</td></tr><tr><td><i>address</i></td><td>Dynamic address object.</td></tr></table>				Option	Description	<i>ip</i>	Standard IPv4 address.	<i>address</i>	Dynamic address object.		
	Option	Description										
	<i>ip</i>	Standard IPv4 address.										
<i>address</i>	Dynamic address object.											
address	Dynamic address of the real server.	string	Maximum length: 79									
ip	IP address of the real server.	user	Not Specified									
port	Port for communicating with the real server. Required if port forwarding is enabled.	integer	Minimum value: 1 Maximum value: 65535	0								
status	Set the status of the real server to active so that it can accept traffic, or on standby or disabled so no traffic is sent.	option	-	active								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>active</i></td><td>Server status active.</td></tr><tr><td><i>standby</i></td><td>Server status standby.</td></tr><tr><td><i>disable</i></td><td>Server status disable.</td></tr></table>				Option	Description	<i>active</i>	Server status active.	<i>standby</i>	Server status standby.	<i>disable</i>	Server status disable.
	Option	Description										
	<i>active</i>	Server status active.										
	<i>standby</i>	Server status standby.										
<i>disable</i>	Server status disable.											
weight	Weight of the real server. If weighted load balancing is enabled, the server with the highest weight gets more connections.	integer	Minimum value: 1 Maximum value: 255	1								
holddown-interval	Time in seconds that the health check monitor continues to monitor and unresponsive server that should be active.	integer	Minimum value: 30 Maximum value: 65535	300								
healthcheck	Enable to check the responsiveness of the real server before forwarding traffic.	option	-	vip								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable per server health check.</td></tr><tr><td><i>enable</i></td><td>Enable per server health check.</td></tr><tr><td><i>vip</i></td><td>Use health check defined in VIP.</td></tr></table>				Option	Description	<i>disable</i>	Disable per server health check.	<i>enable</i>	Enable per server health check.	<i>vip</i>	Use health check defined in VIP.
	Option	Description										
	<i>disable</i>	Disable per server health check.										
	<i>enable</i>	Enable per server health check.										
<i>vip</i>	Use health check defined in VIP.											
http-host	HTTP server domain name in HTTP header.	string	Maximum length: 63									

Parameter	Description	Type	Size	Default
max-connections	Max number of active connections that can be directed to the real server. When reached, sessions are sent to other real servers.	integer	Minimum value: 0 Maximum value: 2147483647	0
monitor <name>	Name of the health check monitor to use when polling to determine a virtual server's connectivity status. Health monitor name.	string	Maximum length: 79	
client-ip	Only clients in this IP range can connect to this real server.	user	Not Specified	

### config ssl-cipher-suites

Parameter	Description	Type	Size	Default
priority	SSL/TLS cipher suites priority.	integer	Minimum value: 0 Maximum value: 4294967295	0
cipher	Cipher suite name.	option	-	

Option	Description
<i>TLS-AES-128-GCM-SHA256</i>	Cipher suite TLS-AES-128-GCM-SHA256.
<i>TLS-AES-256-GCM-SHA384</i>	Cipher suite TLS-AES-256-GCM-SHA384.
<i>TLS-CHACHA20-POLY1305-SHA256</i>	Cipher suite TLS-CHACHA20-POLY1305-SHA256.
<i>TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256</i>	Cipher suite TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256.

Parameter	Description	Type	Size	Default																								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256</i></td><td>Cipher suite TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256.</td></tr><tr><td><i>TLS-DHE-RSA-WITH-CHACHA20-POLY1305-SHA256</i></td><td>Cipher suite TLS-DHE-RSA-WITH-CHACHA20-POLY1305-SHA256.</td></tr><tr><td><i>TLS-DHE-RSA-WITH-AES-128-CBC-SHA</i></td><td>Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA.</td></tr><tr><td><i>TLS-DHE-RSA-WITH-AES-256-CBC-SHA</i></td><td>Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA.</td></tr><tr><td><i>TLS-DHE-RSA-WITH-AES-128-CBC-SHA256</i></td><td>Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA256.</td></tr><tr><td><i>TLS-DHE-RSA-WITH-AES-128-GCM-SHA256</i></td><td>Cipher suite TLS-DHE-RSA-WITH-AES-128-GCM-SHA256.</td></tr><tr><td><i>TLS-DHE-RSA-WITH-AES-256-CBC-SHA256</i></td><td>Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA256.</td></tr><tr><td><i>TLS-DHE-RSA-WITH-AES-256-GCM-SHA384</i></td><td>Cipher suite TLS-DHE-RSA-WITH-AES-256-GCM-SHA384.</td></tr><tr><td><i>TLS-DHE-DSS-WITH-AES-128-CBC-SHA</i></td><td>Cipher suite TLS-DHE-DSS-WITH-AES-128-CBC-SHA.</td></tr><tr><td><i>TLS-DHE-DSS-WITH-AES-256-CBC-SHA</i></td><td>Cipher suite TLS-DHE-DSS-WITH-AES-256-CBC-SHA.</td></tr><tr><td><i>TLS-DHE-DSS-WITH-AES-128-CBC-SHA256</i></td><td>Cipher suite TLS-DHE-DSS-WITH-AES-128-CBC-SHA256.</td></tr></table>	Option	Description	<i>TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256.	<i>TLS-DHE-RSA-WITH-CHACHA20-POLY1305-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-CHACHA20-POLY1305-SHA256.	<i>TLS-DHE-RSA-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA.	<i>TLS-DHE-RSA-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA.	<i>TLS-DHE-RSA-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA256.	<i>TLS-DHE-RSA-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-AES-128-GCM-SHA256.	<i>TLS-DHE-RSA-WITH-AES-256-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA256.	<i>TLS-DHE-RSA-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-DHE-RSA-WITH-AES-256-GCM-SHA384.	<i>TLS-DHE-DSS-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-AES-128-CBC-SHA.	<i>TLS-DHE-DSS-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-AES-256-CBC-SHA.	<i>TLS-DHE-DSS-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-AES-128-CBC-SHA256.			
Option	Description																											
<i>TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256.																											
<i>TLS-DHE-RSA-WITH-CHACHA20-POLY1305-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-CHACHA20-POLY1305-SHA256.																											
<i>TLS-DHE-RSA-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA.																											
<i>TLS-DHE-RSA-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA.																											
<i>TLS-DHE-RSA-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA256.																											
<i>TLS-DHE-RSA-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-AES-128-GCM-SHA256.																											
<i>TLS-DHE-RSA-WITH-AES-256-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA256.																											
<i>TLS-DHE-RSA-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-DHE-RSA-WITH-AES-256-GCM-SHA384.																											
<i>TLS-DHE-DSS-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-AES-128-CBC-SHA.																											
<i>TLS-DHE-DSS-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-AES-256-CBC-SHA.																											
<i>TLS-DHE-DSS-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-AES-128-CBC-SHA256.																											



Parameter	Description	Type	Size	Default
	Option	Description		
	TLS-DHE-DSS-WITH-AES-128-GCM-SHA256	Cipher suite TLS-DHE-DSS-WITH-AES-128-GCM-SHA256.		
	TLS-DHE-DSS-WITH-AES-256-CBC-SHA256	Cipher suite TLS-DHE-DSS-WITH-AES-256-CBC-SHA256.		
	TLS-DHE-DSS-WITH-AES-256-GCM-SHA384	Cipher suite TLS-DHE-DSS-WITH-AES-256-GCM-SHA384.		
	TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA	Cipher suite TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA.		
	TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA256	Cipher suite TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA256.		
	TLS-ECDHE-RSA-WITH-AES-128-GCM-SHA256	Cipher suite TLS-ECDHE-RSA-WITH-AES-128-GCM-SHA256.		
	TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA	Cipher suite TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA.		
	TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA384	Cipher suite TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA384.		
	TLS-ECDHE-RSA-WITH-AES-256-GCM-SHA384	Cipher suite TLS-ECDHE-RSA-WITH-AES-256-GCM-SHA384.		
TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA.			

Parameter	Description	Type	Size	Default																								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA256</i></td><td>Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA256.</td></tr><tr><td><i>TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256</i></td><td>Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256.</td></tr><tr><td><i>TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA</i></td><td>Cipher suite TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA.</td></tr><tr><td><i>TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA384</i></td><td>Cipher suite TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA384.</td></tr><tr><td><i>TLS-ECDHE-ECDSA-WITH-AES-256-GCM-SHA384</i></td><td>Cipher suite TLS-ECDHE-ECDSA-WITH-AES-256-GCM-SHA384.</td></tr><tr><td><i>TLS-RSA-WITH-AES-128-CBC-SHA</i></td><td>Cipher suite TLS-RSA-WITH-AES-128-CBC-SHA.</td></tr><tr><td><i>TLS-RSA-WITH-AES-256-CBC-SHA</i></td><td>Cipher suite TLS-RSA-WITH-AES-256-CBC-SHA.</td></tr><tr><td><i>TLS-RSA-WITH-AES-128-CBC-SHA256</i></td><td>Cipher suite TLS-RSA-WITH-AES-128-CBC-SHA256.</td></tr><tr><td><i>TLS-RSA-WITH-AES-128-GCM-SHA256</i></td><td>Cipher suite TLS-RSA-WITH-AES-128-GCM-SHA256.</td></tr><tr><td><i>TLS-RSA-WITH-AES-256-CBC-SHA256</i></td><td>Cipher suite TLS-RSA-WITH-AES-256-CBC-SHA256.</td></tr><tr><td><i>TLS-RSA-WITH-AES-256-GCM-SHA384</i></td><td>Cipher suite TLS-RSA-WITH-AES-256-GCM-SHA384.</td></tr></table>	Option	Description	<i>TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA256.	<i>TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256.	<i>TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA.	<i>TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA384.	<i>TLS-ECDHE-ECDSA-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-256-GCM-SHA384.	<i>TLS-RSA-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-AES-128-CBC-SHA.	<i>TLS-RSA-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-AES-256-CBC-SHA.	<i>TLS-RSA-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-AES-128-CBC-SHA256.	<i>TLS-RSA-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-RSA-WITH-AES-128-GCM-SHA256.	<i>TLS-RSA-WITH-AES-256-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-AES-256-CBC-SHA256.	<i>TLS-RSA-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-RSA-WITH-AES-256-GCM-SHA384.			
Option	Description																											
<i>TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA256.																											
<i>TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256.																											
<i>TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA.																											
<i>TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA384.																											
<i>TLS-ECDHE-ECDSA-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-256-GCM-SHA384.																											
<i>TLS-RSA-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-AES-128-CBC-SHA.																											
<i>TLS-RSA-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-AES-256-CBC-SHA.																											
<i>TLS-RSA-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-AES-128-CBC-SHA256.																											
<i>TLS-RSA-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-RSA-WITH-AES-128-GCM-SHA256.																											
<i>TLS-RSA-WITH-AES-256-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-AES-256-CBC-SHA256.																											
<i>TLS-RSA-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-RSA-WITH-AES-256-GCM-SHA384.																											

Parameter	Description	Type	Size	Default
	Option	Description		
	TLS-RSA-WITH-CAMELLIA-128-CBC-SHA	Cipher suite TLS-RSA-WITH-CAMELLIA-128-CBC-SHA.		
	TLS-RSA-WITH-CAMELLIA-256-CBC-SHA	Cipher suite TLS-RSA-WITH-CAMELLIA-256-CBC-SHA.		
	TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256	Cipher suite TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256.		
	TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256	Cipher suite TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256.		
	TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA	Cipher suite TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA.		
	TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA.		
	TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA	Cipher suite TLS-DSS-RSA-WITH-CAMELLIA-128-CBC-SHA.		
	TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA.		
	TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA.		
TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA256	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA256.			

Parameter	Description	Type	Size	Default																										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256</td><td>Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256.</td></tr><tr><td>TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256</td><td>Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256.</td></tr><tr><td>TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256</td><td>Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256.</td></tr><tr><td>TLS-DHE-RSA-WITH-SEED-CBC-SHA</td><td>Cipher suite TLS-DHE-RSA-WITH-SEED-CBC-SHA.</td></tr><tr><td>TLS-DHE-DSS-WITH-SEED-CBC-SHA</td><td>Cipher suite TLS-DHE-DSS-WITH-SEED-CBC-SHA.</td></tr><tr><td>TLS-DHE-RSA-WITH-ARIA-128-CBC-SHA256</td><td>Cipher suite TLS-DHE-RSA-WITH-ARIA-128-CBC-SHA256.</td></tr><tr><td>TLS-DHE-RSA-WITH-ARIA-256-CBC-SHA384</td><td>Cipher suite TLS-DHE-RSA-WITH-ARIA-256-CBC-SHA384.</td></tr><tr><td>TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256</td><td>Cipher suite TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256.</td></tr><tr><td>TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384</td><td>Cipher suite TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384.</td></tr><tr><td>TLS-RSA-WITH-SEED-CBC-SHA</td><td>Cipher suite TLS-RSA-WITH-SEED-CBC-SHA.</td></tr><tr><td>TLS-RSA-WITH-ARIA-128-CBC-SHA256</td><td>Cipher suite TLS-RSA-WITH-ARIA-128-CBC-SHA256.</td></tr><tr><td>TLS-RSA-WITH-ARIA-256-CBC-SHA384</td><td>Cipher suite TLS-RSA-WITH-ARIA-256-CBC-SHA384.</td></tr></table>	Option	Description	TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256.	TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256.	TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256.	TLS-DHE-RSA-WITH-SEED-CBC-SHA	Cipher suite TLS-DHE-RSA-WITH-SEED-CBC-SHA.	TLS-DHE-DSS-WITH-SEED-CBC-SHA	Cipher suite TLS-DHE-DSS-WITH-SEED-CBC-SHA.	TLS-DHE-RSA-WITH-ARIA-128-CBC-SHA256	Cipher suite TLS-DHE-RSA-WITH-ARIA-128-CBC-SHA256.	TLS-DHE-RSA-WITH-ARIA-256-CBC-SHA384	Cipher suite TLS-DHE-RSA-WITH-ARIA-256-CBC-SHA384.	TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256	Cipher suite TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256.	TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384	Cipher suite TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384.	TLS-RSA-WITH-SEED-CBC-SHA	Cipher suite TLS-RSA-WITH-SEED-CBC-SHA.	TLS-RSA-WITH-ARIA-128-CBC-SHA256	Cipher suite TLS-RSA-WITH-ARIA-128-CBC-SHA256.	TLS-RSA-WITH-ARIA-256-CBC-SHA384	Cipher suite TLS-RSA-WITH-ARIA-256-CBC-SHA384.			
Option	Description																													
TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256.																													
TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256.																													
TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256.																													
TLS-DHE-RSA-WITH-SEED-CBC-SHA	Cipher suite TLS-DHE-RSA-WITH-SEED-CBC-SHA.																													
TLS-DHE-DSS-WITH-SEED-CBC-SHA	Cipher suite TLS-DHE-DSS-WITH-SEED-CBC-SHA.																													
TLS-DHE-RSA-WITH-ARIA-128-CBC-SHA256	Cipher suite TLS-DHE-RSA-WITH-ARIA-128-CBC-SHA256.																													
TLS-DHE-RSA-WITH-ARIA-256-CBC-SHA384	Cipher suite TLS-DHE-RSA-WITH-ARIA-256-CBC-SHA384.																													
TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256	Cipher suite TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256.																													
TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384	Cipher suite TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384.																													
TLS-RSA-WITH-SEED-CBC-SHA	Cipher suite TLS-RSA-WITH-SEED-CBC-SHA.																													
TLS-RSA-WITH-ARIA-128-CBC-SHA256	Cipher suite TLS-RSA-WITH-ARIA-128-CBC-SHA256.																													
TLS-RSA-WITH-ARIA-256-CBC-SHA384	Cipher suite TLS-RSA-WITH-ARIA-256-CBC-SHA384.																													

Parameter	Description	Type	Size	Default
	Option	Description		
	TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256	Cipher suite TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256.		
	TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384	Cipher suite TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384.		
	TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC-SHA256	Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC_SHA256.		
	TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC-SHA384	Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC_SHA384.		
	TLS-ECDHE-RSA-WITH-RC4-128-SHA	Cipher suite TLS-ECDHE-RSA-WITH-RC4-128-SHA.		
	TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA	Cipher suite TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA.		
	TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA	Cipher suite TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA.		
	TLS-RSA-WITH-3DES-EDE-CBC-SHA	Cipher suite TLS-RSA-WITH-3DES-EDE-CBC-SHA.		
	TLS-RSA-WITH-RC4-128-MD5	Cipher suite TLS-RSA-WITH-RC4-128-MD5.		
	TLS-RSA-WITH-RC4-128-SHA	Cipher suite TLS-RSA-WITH-RC4-128-SHA.		
TLS-DHE-RSA-WITH-DES-CBC-SHA	Cipher suite TLS-DHE-RSA-WITH-DES-CBC-SHA.			

Parameter	Description	Type	Size	Default												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>TLS-DHE-DSS-WITH-DES-CBC-SHA</i></td><td>Cipher suite TLS-DHE-DSS-WITH-DES-CBC-SHA.</td></tr><tr><td><i>TLS-RSA-WITH-DES-CBC-SHA</i></td><td>Cipher suite TLS-RSA-WITH-DES-CBC-SHA.</td></tr></table>	Option	Description	<i>TLS-DHE-DSS-WITH-DES-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-DES-CBC-SHA.	<i>TLS-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-DES-CBC-SHA.									
	Option	Description														
	<i>TLS-DHE-DSS-WITH-DES-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-DES-CBC-SHA.														
<i>TLS-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-DES-CBC-SHA.															
versions	SSL/TLS versions that the cipher suite can be used with.	option	-	ssl-3.0 tls-1.0 tls-1.1 tls-1.2 tls-1.3												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ssl-3.0</i></td><td>SSL 3.0.</td></tr><tr><td><i>tls-1.0</i></td><td>TLS 1.0.</td></tr><tr><td><i>tls-1.1</i></td><td>TLS 1.1.</td></tr><tr><td><i>tls-1.2</i></td><td>TLS 1.2.</td></tr><tr><td><i>tls-1.3</i></td><td>TLS 1.3.</td></tr></table>	Option	Description	<i>ssl-3.0</i>	SSL 3.0.	<i>tls-1.0</i>	TLS 1.0.	<i>tls-1.1</i>	TLS 1.1.	<i>tls-1.2</i>	TLS 1.2.	<i>tls-1.3</i>	TLS 1.3.			
	Option	Description														
	<i>ssl-3.0</i>	SSL 3.0.														
	<i>tls-1.0</i>	TLS 1.0.														
	<i>tls-1.1</i>	TLS 1.1.														
	<i>tls-1.2</i>	TLS 1.2.														
<i>tls-1.3</i>	TLS 1.3.															

### config ssl-server-cipher-suites

Parameter	Description	Type	Size	Default								
priority	SSL/TLS cipher suites priority.	integer	Minimum value: 0 Maximum value: 4294967295	0								
cipher	Cipher suite name.	option	-									
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>TLS-AES-128-GCM-SHA256</td><td>Cipher suite TLS-AES-128-GCM-SHA256.</td></tr><tr><td>TLS-AES-256-GCM-SHA384</td><td>Cipher suite TLS-AES-256-GCM-SHA384.</td></tr><tr><td>TLS-CHACHA20-POLY1305-SHA256</td><td>Cipher suite TLS-CHACHA20-POLY1305-SHA256.</td></tr></table>	Option	Description	TLS-AES-128-GCM-SHA256	Cipher suite TLS-AES-128-GCM-SHA256.	TLS-AES-256-GCM-SHA384	Cipher suite TLS-AES-256-GCM-SHA384.	TLS-CHACHA20-POLY1305-SHA256	Cipher suite TLS-CHACHA20-POLY1305-SHA256.			
Option	Description											
TLS-AES-128-GCM-SHA256	Cipher suite TLS-AES-128-GCM-SHA256.											
TLS-AES-256-GCM-SHA384	Cipher suite TLS-AES-256-GCM-SHA384.											
TLS-CHACHA20-POLY1305-SHA256	Cipher suite TLS-CHACHA20-POLY1305-SHA256.											

Parameter	Description	Type	Size	Default
	Option	Description		
	TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256	Cipher suite TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256.		
	TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256	Cipher suite TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256.		
	TLS-DHE-RSA-WITH-CHACHA20-POLY1305-SHA256	Cipher suite TLS-DHE-RSA-WITH-CHACHA20-POLY1305-SHA256.		
	TLS-DHE-RSA-WITH-AES-128-CBC-SHA	Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA.		
	TLS-DHE-RSA-WITH-AES-256-CBC-SHA	Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA.		
	TLS-DHE-RSA-WITH-AES-128-CBC-SHA256	Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA256.		
	TLS-DHE-RSA-WITH-AES-128-GCM-SHA256	Cipher suite TLS-DHE-RSA-WITH-AES-128-GCM-SHA256.		
	TLS-DHE-RSA-WITH-AES-256-CBC-SHA256	Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA256.		
	TLS-DHE-RSA-WITH-AES-256-GCM-SHA384	Cipher suite TLS-DHE-RSA-WITH-AES-256-GCM-SHA384.		
TLS-DHE-DSS-WITH-AES-128-CBC-SHA	Cipher suite TLS-DHE-DSS-WITH-AES-128-CBC-SHA.			

Parameter	Description	Type	Size	Default
	Option	Description		
	TLS-DHE-DSS-WITH-AES-256-CBC-SHA	Cipher suite TLS-DHE-DSS-WITH-AES-256-CBC-SHA.		
	TLS-DHE-DSS-WITH-AES-128-CBC-SHA256	Cipher suite TLS-DHE-DSS-WITH-AES-128-CBC-SHA256.		
	TLS-DHE-DSS-WITH-AES-128-GCM-SHA256	Cipher suite TLS-DHE-DSS-WITH-AES-128-GCM-SHA256.		
	TLS-DHE-DSS-WITH-AES-256-CBC-SHA256	Cipher suite TLS-DHE-DSS-WITH-AES-256-CBC-SHA256.		
	TLS-DHE-DSS-WITH-AES-256-GCM-SHA384	Cipher suite TLS-DHE-DSS-WITH-AES-256-GCM-SHA384.		
	TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA	Cipher suite TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA.		
	TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA256	Cipher suite TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA256.		
	TLS-ECDHE-RSA-WITH-AES-128-GCM-SHA256	Cipher suite TLS-ECDHE-RSA-WITH-AES-128-GCM-SHA256.		
	TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA	Cipher suite TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA.		
	TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA384	Cipher suite TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA384.		
	TLS-ECDHE-RSA-WITH-AES-256-GCM-SHA384	Cipher suite TLS-ECDHE-RSA-WITH-AES-256-GCM-SHA384.		



Parameter	Description	Type	Size	Default
	Option	Description		
	TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA.		
	TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA256	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA256.		
	TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256.		
	TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA.		
	TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA384	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA384.		
	TLS-ECDHE-ECDSA-WITH-AES-256-GCM-SHA384	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-256-GCM-SHA384.		
	TLS-RSA-WITH-AES-128-CBC-SHA	Cipher suite TLS-RSA-WITH-AES-128-CBC-SHA.		
	TLS-RSA-WITH-AES-256-CBC-SHA	Cipher suite TLS-RSA-WITH-AES-256-CBC-SHA.		
	TLS-RSA-WITH-AES-128-CBC-SHA256	Cipher suite TLS-RSA-WITH-AES-128-CBC-SHA256.		
TLS-RSA-WITH-AES-128-GCM-SHA256	Cipher suite TLS-RSA-WITH-AES-128-GCM-SHA256.			

Parameter	Description	Type	Size	Default
	Option	Description		
	TLS-RSA-WITH-AES-256-CBC-SHA256	Cipher suite TLS-RSA-WITH-AES-256-CBC-SHA256.		
	TLS-RSA-WITH-AES-256-GCM-SHA384	Cipher suite TLS-RSA-WITH-AES-256-GCM-SHA384.		
	TLS-RSA-WITH-CAMELLIA-128-CBC-SHA	Cipher suite TLS-RSA-WITH-CAMELLIA-128-CBC-SHA.		
	TLS-RSA-WITH-CAMELLIA-256-CBC-SHA	Cipher suite TLS-RSA-WITH-CAMELLIA-256-CBC-SHA.		
	TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256	Cipher suite TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256.		
	TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256	Cipher suite TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256.		
	TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA	Cipher suite TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA.		
	TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA.		
	TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA	Cipher suite TLS-DSS-RSA-WITH-CAMELLIA-128-CBC-SHA.		
	TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA.		
	TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA.		

Parameter	Description	Type	Size	Default
	Option	Description		
	TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA256	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA256.		
	TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256.		
	TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256.		
	TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256.		
	TLS-DHE-RSA-WITH-SEED-CBC-SHA	Cipher suite TLS-DHE-RSA-WITH-SEED-CBC-SHA.		
	TLS-DHE-DSS-WITH-SEED-CBC-SHA	Cipher suite TLS-DHE-DSS-WITH-SEED-CBC-SHA.		
	TLS-DHE-RSA-WITH-ARIA-128-CBC-SHA256	Cipher suite TLS-DHE-RSA-WITH-ARIA-128-CBC-SHA256.		
	TLS-DHE-RSA-WITH-ARIA-256-CBC-SHA384	Cipher suite TLS-DHE-RSA-WITH-ARIA-256-CBC-SHA384.		
	TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256	Cipher suite TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256.		
	TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384	Cipher suite TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384.		
	TLS-RSA-WITH-SEED-CBC-SHA	Cipher suite TLS-RSA-WITH-SEED-CBC-SHA.		

Parameter	Description	Type	Size	Default																								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>TLS-RSA-WITH-ARIA-128-CBC-SHA256</i></td><td>Cipher suite TLS-RSA-WITH-ARIA-128-CBC-SHA256.</td></tr><tr><td><i>TLS-RSA-WITH-ARIA-256-CBC-SHA384</i></td><td>Cipher suite TLS-RSA-WITH-ARIA-256-CBC-SHA384.</td></tr><tr><td><i>TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256</i></td><td>Cipher suite TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256.</td></tr><tr><td><i>TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384</i></td><td>Cipher suite TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384.</td></tr><tr><td><i>TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC-SHA256</i></td><td>Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC_SHA256.</td></tr><tr><td><i>TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC-SHA384</i></td><td>Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC_SHA384.</td></tr><tr><td><i>TLS-ECDHE-RSA-WITH-RC4-128-SHA</i></td><td>Cipher suite TLS-ECDHE-RSA-WITH-RC4-128-SHA.</td></tr><tr><td><i>TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA</i></td><td>Cipher suite TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA.</td></tr><tr><td><i>TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA</i></td><td>Cipher suite TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA.</td></tr><tr><td><i>TLS-RSA-WITH-3DES-EDE-CBC-SHA</i></td><td>Cipher suite TLS-RSA-WITH-3DES-EDE-CBC-SHA.</td></tr><tr><td><i>TLS-RSA-WITH-RC4-128-MD5</i></td><td>Cipher suite TLS-RSA-WITH-RC4-128-MD5.</td></tr></table>	Option	Description	<i>TLS-RSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-ARIA-128-CBC-SHA256.	<i>TLS-RSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-RSA-WITH-ARIA-256-CBC-SHA384.	<i>TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256.	<i>TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384.	<i>TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC_SHA256.	<i>TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC_SHA384.	<i>TLS-ECDHE-RSA-WITH-RC4-128-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-RC4-128-SHA.	<i>TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA.	<i>TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA.	<i>TLS-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-3DES-EDE-CBC-SHA.	<i>TLS-RSA-WITH-RC4-128-MD5</i>	Cipher suite TLS-RSA-WITH-RC4-128-MD5.			
Option	Description																											
<i>TLS-RSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-ARIA-128-CBC-SHA256.																											
<i>TLS-RSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-RSA-WITH-ARIA-256-CBC-SHA384.																											
<i>TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256.																											
<i>TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384.																											
<i>TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC_SHA256.																											
<i>TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC_SHA384.																											
<i>TLS-ECDHE-RSA-WITH-RC4-128-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-RC4-128-SHA.																											
<i>TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA.																											
<i>TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA.																											
<i>TLS-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-3DES-EDE-CBC-SHA.																											
<i>TLS-RSA-WITH-RC4-128-MD5</i>	Cipher suite TLS-RSA-WITH-RC4-128-MD5.																											

Parameter	Description	Type	Size	Default												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>TLS-RSA-WITH-RC4-128-SHA</i></td><td>Cipher suite TLS-RSA-WITH-RC4-128-SHA.</td></tr><tr><td><i>TLS-DHE-RSA-WITH-DES-CBC-SHA</i></td><td>Cipher suite TLS-DHE-RSA-WITH-DES-CBC-SHA.</td></tr><tr><td><i>TLS-DHE-DSS-WITH-DES-CBC-SHA</i></td><td>Cipher suite TLS-DHE-DSS-WITH-DES-CBC-SHA.</td></tr><tr><td><i>TLS-RSA-WITH-DES-CBC-SHA</i></td><td>Cipher suite TLS-RSA-WITH-DES-CBC-SHA.</td></tr></table>	Option	Description	<i>TLS-RSA-WITH-RC4-128-SHA</i>	Cipher suite TLS-RSA-WITH-RC4-128-SHA.	<i>TLS-DHE-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-DES-CBC-SHA.	<i>TLS-DHE-DSS-WITH-DES-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-DES-CBC-SHA.	<i>TLS-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-DES-CBC-SHA.					
	Option	Description														
	<i>TLS-RSA-WITH-RC4-128-SHA</i>	Cipher suite TLS-RSA-WITH-RC4-128-SHA.														
	<i>TLS-DHE-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-DES-CBC-SHA.														
	<i>TLS-DHE-DSS-WITH-DES-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-DES-CBC-SHA.														
<i>TLS-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-DES-CBC-SHA.															
versions	SSL/TLS versions that the cipher suite can be used with.	option	-	ssl-3.0 tls-1.0 tls-1.1 tls-1.2 tls-1.3												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ssl-3.0</i></td><td>SSL 3.0.</td></tr><tr><td><i>tls-1.0</i></td><td>TLS 1.0.</td></tr><tr><td><i>tls-1.1</i></td><td>TLS 1.1.</td></tr><tr><td><i>tls-1.2</i></td><td>TLS 1.2.</td></tr><tr><td><i>tls-1.3</i></td><td>TLS 1.3.</td></tr></table>	Option	Description	<i>ssl-3.0</i>	SSL 3.0.	<i>tls-1.0</i>	TLS 1.0.	<i>tls-1.1</i>	TLS 1.1.	<i>tls-1.2</i>	TLS 1.2.	<i>tls-1.3</i>	TLS 1.3.			
	Option	Description														
	<i>ssl-3.0</i>	SSL 3.0.														
	<i>tls-1.0</i>	TLS 1.0.														
	<i>tls-1.1</i>	TLS 1.1.														
	<i>tls-1.2</i>	TLS 1.2.														
<i>tls-1.3</i>	TLS 1.3.															

## config firewall vip6

Configure virtual IP for IPv6.

```
config firewall vip6
  Description: Configure virtual IP for IPv6.
  edit <name>
    set add-nat64-route [disable|enable]
    set color {integer}
    set comment {var-string}
    set embedded-ipv4-address [disable|enable]
    set extip {user}
    set extport {user}
    set http-cookie-age {integer}
    set http-cookie-domain {string}
    set http-cookie-domain-from-host [disable|enable]
    set http-cookie-generation {integer}
    set http-cookie-path {string}
    set http-cookie-share [disable|same-ip]
    set http-ip-header [enable|disable]
```

```

set http-ip-header-name {string}
set http-multiplex [enable|disable]
set http-redirect [enable|disable]
set https-cookie-secure [disable|enable]
set id {integer}
set ipv4-mappedip {user}
set ipv4-mappedport {user}
set ldb-method [static|round-robin|...]
set mappedip {user}
set mappedport {user}
set max-embryonic-connections {integer}
set monitor <name1>, <name2>, ...
set nat-source-vip [disable|enable]
set nat64 [disable|enable]
set nat66 [disable|enable]
set ndp-reply [disable|enable]
set outlook-web-access [disable|enable]
set persistence [none|http-cookie|...]
set portforward [disable|enable]
set protocol [tcp|udp|...]
config realservers
    Description: Select the real servers that this server load balancing VIP will
distribute traffic to.
    edit <id>
        set ip {user}
        set port {integer}
        set status [active|standby|...]
        set weight {integer}
        set holddown-interval {integer}
        set healthcheck [disable|enable|...]
        set http-host {string}
        set max-connections {integer}
        set monitor <name1>, <name2>, ...
        set client-ip {user}
    next
end
set server-type [http|https|...]
set src-filter <range1>, <range2>, ...
set ssl-accept-ffdhe-groups [enable|disable]
set ssl-algorithm [high|medium|...]
set ssl-certificate {string}
config ssl-cipher-suites
    Description: SSL/TLS cipher suites acceptable from a client, ordered by
priority.
    edit <priority>
        set cipher [TLS-AES-128-GCM-SHA256|TLS-AES-256-GCM-SHA384|...]
        set versions {option1}, {option2}, ...
    next
end
set ssl-client-fallback [disable|enable]
set ssl-client-rekey-count {integer}
set ssl-client-renegotiation [allow|deny|...]
set ssl-client-session-state-max {integer}
set ssl-client-session-state-timeout {integer}
set ssl-client-session-state-type [disable|time|...]
set ssl-dh-bits [768|1024|...]

```

```

set ssl-hpkp [disable|enable|...]
set ssl-hpkp-age {integer}
set ssl-hpkp-backup {string}
set ssl-hpkp-include-subdomains [disable|enable]
set ssl-hpkp-primary {string}
set ssl-hpkp-report-uri {var-string}
set ssl-hsts [disable|enable]
set ssl-hsts-age {integer}
set ssl-hsts-include-subdomains [disable|enable]
set ssl-http-location-conversion [enable|disable]
set ssl-http-match-host [enable|disable]
set ssl-max-version [ssl-3.0|tls-1.0|...]
set ssl-min-version [ssl-3.0|tls-1.0|...]
set ssl-mode [half|full]
set ssl-pfs [require|deny|...]
set ssl-send-empty-frags [enable|disable]
set ssl-server-algorithm [high|medium|...]
config ssl-server-cipher-suites
    Description: SSL/TLS cipher suites to offer to a server, ordered by priority.
    edit <priority>
        set cipher [TLS-AES-128-GCM-SHA256|TLS-AES-256-GCM-SHA384|...]
        set versions {option1}, {option2}, ...
    next
end
set ssl-server-max-version [ssl-3.0|tls-1.0|...]
set ssl-server-min-version [ssl-3.0|tls-1.0|...]
set ssl-server-session-state-max {integer}
set ssl-server-session-state-timeout {integer}
set ssl-server-session-state-type [disable|time|...]
set type [static-nat|server-load-balance|...]
set uuid {uuid}
set weblogic-server [disable|enable]
set websphere-server [disable|enable]
next
end

```

## config firewall vip6

Parameter	Description	Type	Size	Default						
add-nat64-route	Enable/disable adding NAT64 route.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable adding NAT64 route.</td></tr><tr><td><i>enable</i></td><td>Enable adding NAT64 route.</td></tr></table>				Option	Description	<i>disable</i>	Disable adding NAT64 route.	<i>enable</i>	Enable adding NAT64 route.
	Option	Description								
	<i>disable</i>	Disable adding NAT64 route.								
<i>enable</i>	Enable adding NAT64 route.									
color	Color of icon on the GUI.	integer	Minimum value: 0 Maximum value: 32	0						

Parameter	Description	Type	Size	Default						
comment	Comment.	var-string	Maximum length: 255							
embedded-ipv4-address	Enable/disable use of the lower 32 bits of the external IPv6 address as mapped IPv4 address.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable use of the lower 32 bits of the external IPv6 address as mapped IPv4 address.</td></tr><tr><td><i>enable</i></td><td>Enable use of the lower 32 bits of the external IPv6 address as mapped IPv4 address.</td></tr></table>	Option	Description	<i>disable</i>	Disable use of the lower 32 bits of the external IPv6 address as mapped IPv4 address.	<i>enable</i>	Enable use of the lower 32 bits of the external IPv6 address as mapped IPv4 address.			
Option	Description									
<i>disable</i>	Disable use of the lower 32 bits of the external IPv6 address as mapped IPv4 address.									
<i>enable</i>	Enable use of the lower 32 bits of the external IPv6 address as mapped IPv4 address.									
extip	IPv6 address or address range on the external interface that you want to map to an address or address range on the destination network.	user	Not Specified							
extport	Incoming port number range that you want to map to a port number range on the destination network.	user	Not Specified							
http-cookie-age	Time in minutes that client web browsers should keep a cookie. Default is 60 minutes. 0 = no time limit.	integer	Minimum value: 0 Maximum value: 525600	60						
http-cookie-domain	Domain that HTTP cookie persistence should apply to.	string	Maximum length: 35							
http-cookie-domain-from-host	Enable/disable use of HTTP cookie domain from host field in HTTP.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable use of HTTP cookie domain from host field in HTTP (use http-cookies-domain setting).</td></tr><tr><td><i>enable</i></td><td>Enable use of HTTP cookie domain from host field in HTTP.</td></tr></table>	Option	Description	<i>disable</i>	Disable use of HTTP cookie domain from host field in HTTP (use http-cookies-domain setting).	<i>enable</i>	Enable use of HTTP cookie domain from host field in HTTP.			
Option	Description									
<i>disable</i>	Disable use of HTTP cookie domain from host field in HTTP (use http-cookies-domain setting).									
<i>enable</i>	Enable use of HTTP cookie domain from host field in HTTP.									
http-cookie-generation	Generation of HTTP cookie to be accepted. Changing invalidates all existing cookies.	integer	Minimum value: 0 Maximum value: 4294967295	0						
http-cookie-path	Limit HTTP cookie persistence to the specified path.	string	Maximum length: 35							



Parameter	Description	Type	Size	Default						
http-cookie-share	Control sharing of cookies across virtual servers. Use of same-ip means a cookie from one virtual server can be used by another. Disable stops cookie sharing.	option	-	same-ip						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Only allow HTTP cookie to match this virtual server.</td></tr><tr><td>same-ip</td><td>Allow HTTP cookie to match any virtual server with same IP.</td></tr></table>	Option	Description	disable	Only allow HTTP cookie to match this virtual server.	same-ip	Allow HTTP cookie to match any virtual server with same IP.			
Option	Description									
disable	Only allow HTTP cookie to match this virtual server.									
same-ip	Allow HTTP cookie to match any virtual server with same IP.									
http-ip-header	For HTTP multiplexing, enable to add the original client IP address in the XForwarded-For HTTP header.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable adding HTTP header.</td></tr><tr><td>disable</td><td>Disable adding HTTP header.</td></tr></table>	Option	Description	enable	Enable adding HTTP header.	disable	Disable adding HTTP header.			
Option	Description									
enable	Enable adding HTTP header.									
disable	Disable adding HTTP header.									
http-ip-header-name	For HTTP multiplexing, enter a custom HTTPS header name. The original client IP address is added to this header. If empty, X-Forwarded-For is used.	string	Maximum length: 35							
http-multiplex	Enable/disable HTTP multiplexing.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable HTTP session multiplexing.</td></tr><tr><td>disable</td><td>Disable HTTP session multiplexing.</td></tr></table>	Option	Description	enable	Enable HTTP session multiplexing.	disable	Disable HTTP session multiplexing.			
Option	Description									
enable	Enable HTTP session multiplexing.									
disable	Disable HTTP session multiplexing.									
http-redirect	Enable/disable redirection of HTTP to HTTPS.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable redirection of HTTP to HTTPS.</td></tr><tr><td>disable</td><td>Disable redirection of HTTP to HTTPS.</td></tr></table>	Option	Description	enable	Enable redirection of HTTP to HTTPS.	disable	Disable redirection of HTTP to HTTPS.			
Option	Description									
enable	Enable redirection of HTTP to HTTPS.									
disable	Disable redirection of HTTP to HTTPS.									
https-cookie-secure	Enable/disable verification that inserted HTTPS cookies are secure.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Do not mark cookie as secure, allow sharing between an HTTP and HTTPS connection.</td></tr><tr><td>enable</td><td>Mark inserted cookie as secure, cookie can only be used for HTTPS a connection.</td></tr></table>	Option	Description	disable	Do not mark cookie as secure, allow sharing between an HTTP and HTTPS connection.	enable	Mark inserted cookie as secure, cookie can only be used for HTTPS a connection.			
Option	Description									
disable	Do not mark cookie as secure, allow sharing between an HTTP and HTTPS connection.									
enable	Mark inserted cookie as secure, cookie can only be used for HTTPS a connection.									

Parameter	Description	Type	Size	Default																
id	Custom defined ID.	integer	Minimum value: 0 Maximum value: 65535	0																
ipv4-mappedip	Range of mapped IP addresses. Specify the start IP address followed by a space and the end IP address.	user	Not Specified																	
ipv4-mappedport	IPv4 port number range on the destination network to which the external port number range is mapped.	user	Not Specified																	
ldb-method	Method used to distribute sessions to real servers.	option	-	static																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>static</i></td><td>Distribute sessions based on source IP.</td></tr><tr><td><i>round-robin</i></td><td>Distribute sessions based round robin order.</td></tr><tr><td><i>weighted</i></td><td>Distribute sessions based on weight.</td></tr><tr><td><i>least-session</i></td><td>Sends new sessions to the server with the lowest session count.</td></tr><tr><td><i>least-rtt</i></td><td>Distribute new sessions to the server with lowest Round-Trip-Time.</td></tr><tr><td><i>first-alive</i></td><td>Distribute sessions to the first server that is alive.</td></tr><tr><td><i>http-host</i></td><td>Distribute sessions to servers based on host field in HTTP header.</td></tr></table>				Option	Description	<i>static</i>	Distribute sessions based on source IP.	<i>round-robin</i>	Distribute sessions based round robin order.	<i>weighted</i>	Distribute sessions based on weight.	<i>least-session</i>	Sends new sessions to the server with the lowest session count.	<i>least-rtt</i>	Distribute new sessions to the server with lowest Round-Trip-Time.	<i>first-alive</i>	Distribute sessions to the first server that is alive.	<i>http-host</i>	Distribute sessions to servers based on host field in HTTP header.
	Option	Description																		
	<i>static</i>	Distribute sessions based on source IP.																		
	<i>round-robin</i>	Distribute sessions based round robin order.																		
	<i>weighted</i>	Distribute sessions based on weight.																		
	<i>least-session</i>	Sends new sessions to the server with the lowest session count.																		
	<i>least-rtt</i>	Distribute new sessions to the server with lowest Round-Trip-Time.																		
	<i>first-alive</i>	Distribute sessions to the first server that is alive.																		
<i>http-host</i>	Distribute sessions to servers based on host field in HTTP header.																			
mappedip	Mapped IPv6 address range in the format startIP-endIP.	user	Not Specified																	
mappedport	Port number range on the destination network to which the external port number range is mapped.	user	Not Specified																	
max-embryonic-connections	Maximum number of incomplete connections.	integer	Minimum value: 0 Maximum value: 100000	1000																
monitor <name>	Name of the health check monitor to use when polling to determine a virtual server's connectivity status. Health monitor name.	string	Maximum length: 79																	
name	Virtual ip6 name.	string	Maximum length: 79																	

Parameter	Description	Type	Size	Default
nat-source-vip	Enable to perform SNAT on traffic from mappedip to the extip for all egress interfaces.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable nat-source-vip.		
	<i>enable</i>	Perform SNAT on traffic from mappedip to the extip for all egress interfaces.		
nat64	Enable/disable DNAT64.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable DNAT64.		
	<i>enable</i>	Enable DNAT64.		
nat66	Enable/disable DNAT66.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable DNAT66.		
	<i>enable</i>	Enable DNAT66.		
ndp-reply	Enable/disable this FortiGate unit's ability to respond to NDP requests for this virtual IP address.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable this FortiGate unit's ability to respond to NDP requests for this virtual IP address.		
	<i>enable</i>	Enable this FortiGate unit's ability to respond to NDP requests for this virtual IP address.		
outlook-web-access	Enable to add the Front-End-Https header for Microsoft Outlook Web Access.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable Outlook Web Access support.		
	<i>enable</i>	Enable Outlook Web Access support.		
persistence	Configure how to make sure that clients connect to the same server every time they make a request that is part of the same session.	option	-	none

Parameter	Description	Type	Size	Default																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>None.</td></tr><tr><td><i>http-cookie</i></td><td>HTTP cookie.</td></tr><tr><td><i>ssl-session-id</i></td><td>SSL session ID.</td></tr></table>	Option	Description	<i>none</i>	None.	<i>http-cookie</i>	HTTP cookie.	<i>ssl-session-id</i>	SSL session ID.															
	Option	Description																						
	<i>none</i>	None.																						
	<i>http-cookie</i>	HTTP cookie.																						
<i>ssl-session-id</i>	SSL session ID.																							
portforward	Enable port forwarding.	option	-	disable																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable port forward.</td></tr><tr><td><i>enable</i></td><td>Enable/disable port forwarding.</td></tr></table>	Option	Description	<i>disable</i>	Disable port forward.	<i>enable</i>	Enable/disable port forwarding.																	
	Option	Description																						
	<i>disable</i>	Disable port forward.																						
<i>enable</i>	Enable/disable port forwarding.																							
protocol	Protocol to use when forwarding packets.	option	-	tcp																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>tcp</i></td><td>TCP.</td></tr><tr><td><i>udp</i></td><td>UDP.</td></tr><tr><td><i>sctp</i></td><td>SCTP.</td></tr></table>	Option	Description	<i>tcp</i>	TCP.	<i>udp</i>	UDP.	<i>sctp</i>	SCTP.															
	Option	Description																						
	<i>tcp</i>	TCP.																						
	<i>udp</i>	UDP.																						
<i>sctp</i>	SCTP.																							
server-type	Protocol to be load balanced by the virtual server (also called the server load balance virtual IP).	option	-																					
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>http</i></td><td>HTTP.</td></tr><tr><td><i>https</i></td><td>HTTPS.</td></tr><tr><td><i>imaps</i></td><td>IMAPS.</td></tr><tr><td><i>pop3s</i></td><td>POP3S.</td></tr><tr><td><i>smtps</i></td><td>SMTPS.</td></tr><tr><td><i>ssl</i></td><td>SSL.</td></tr><tr><td><i>tcp</i></td><td>TCP.</td></tr><tr><td><i>udp</i></td><td>UDP.</td></tr><tr><td><i>ip</i></td><td>IP.</td></tr></table>	Option	Description	<i>http</i>	HTTP.	<i>https</i>	HTTPS.	<i>imaps</i>	IMAPS.	<i>pop3s</i>	POP3S.	<i>smtps</i>	SMTPS.	<i>ssl</i>	SSL.	<i>tcp</i>	TCP.	<i>udp</i>	UDP.	<i>ip</i>	IP.			
	Option	Description																						
	<i>http</i>	HTTP.																						
	<i>https</i>	HTTPS.																						
	<i>imaps</i>	IMAPS.																						
	<i>pop3s</i>	POP3S.																						
	<i>smtps</i>	SMTPS.																						
	<i>ssl</i>	SSL.																						
	<i>tcp</i>	TCP.																						
<i>udp</i>	UDP.																							
<i>ip</i>	IP.																							
src-filter <range>	Source IP6 filter (x:x:x:x:x:x/x). Separate addresses with spaces. Source-filter range.	string	Maximum length: 79																					
ssl-accept-ffdhe-groups	Enable/disable FFDHE cipher suite for SSL key exchange.	option	-	enable																				

Parameter	Description	Type	Size	Default										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Accept FFDHE groups.</td></tr><tr><td><i>disable</i></td><td>Do not accept FFDHE groups.</td></tr></table>	Option	Description	<i>enable</i>	Accept FFDHE groups.	<i>disable</i>	Do not accept FFDHE groups.							
	Option	Description												
	<i>enable</i>	Accept FFDHE groups.												
<i>disable</i>	Do not accept FFDHE groups.													
ssl-algorithm	Permitted encryption algorithms for SSL sessions according to encryption strength.	option	-	high										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>high</i></td><td>Use AES.</td></tr><tr><td><i>medium</i></td><td>Use AES, 3DES, or RC4.</td></tr><tr><td><i>low</i></td><td>Use AES, 3DES, RC4, or DES.</td></tr><tr><td><i>custom</i></td><td>Use config ssl-cipher-suites to select the cipher suites that are allowed.</td></tr></table>	Option	Description	<i>high</i>	Use AES.	<i>medium</i>	Use AES, 3DES, or RC4.	<i>low</i>	Use AES, 3DES, RC4, or DES.	<i>custom</i>	Use config ssl-cipher-suites to select the cipher suites that are allowed.			
	Option	Description												
	<i>high</i>	Use AES.												
	<i>medium</i>	Use AES, 3DES, or RC4.												
	<i>low</i>	Use AES, 3DES, RC4, or DES.												
<i>custom</i>	Use config ssl-cipher-suites to select the cipher suites that are allowed.													
ssl-certificate	The name of the certificate to use for SSL handshake.	string	Maximum length: 35											
ssl-client-fallback	Enable/disable support for preventing Downgrade Attacks on client connections (RFC 7507).	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable.</td></tr><tr><td><i>enable</i></td><td>Enable.</td></tr></table>	Option	Description	<i>disable</i>	Disable.	<i>enable</i>	Enable.							
	Option	Description												
	<i>disable</i>	Disable.												
<i>enable</i>	Enable.													
ssl-client-rekey-count	Maximum length of data in MB before triggering a client rekey (0 = disable).	integer	Minimum value: 200 Maximum value: 1048576	0										
ssl-client-renegotiation	Allow, deny, or require secure renegotiation of client sessions to comply with RFC 5746.	option	-	secure										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow a SSL client to renegotiate.</td></tr><tr><td><i>deny</i></td><td>Abort any SSL connection that attempts to renegotiate.</td></tr><tr><td><i>secure</i></td><td>Reject any SSL connection that does not offer a RFC 5746 Secure Renegotiation Indication.</td></tr></table>	Option	Description	<i>allow</i>	Allow a SSL client to renegotiate.	<i>deny</i>	Abort any SSL connection that attempts to renegotiate.	<i>secure</i>	Reject any SSL connection that does not offer a RFC 5746 Secure Renegotiation Indication.					
	Option	Description												
	<i>allow</i>	Allow a SSL client to renegotiate.												
	<i>deny</i>	Abort any SSL connection that attempts to renegotiate.												
<i>secure</i>	Reject any SSL connection that does not offer a RFC 5746 Secure Renegotiation Indication.													

Parameter	Description	Type	Size	Default														
ssl-client-session-state-max	Maximum number of client to FortiGate SSL session states to keep.	integer	Minimum value: 1 Maximum value: 10000	1000														
ssl-client-session-state-timeout	Number of minutes to keep client to FortiGate SSL session state.	integer	Minimum value: 1 Maximum value: 14400	30														
ssl-client-session-state-type	How to expire SSL sessions for the segment of the SSL connection between the client and the FortiGate.	option	-	both														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Do not keep session states.</td></tr><tr><td>time</td><td>Expire session states after this many minutes.</td></tr><tr><td>count</td><td>Expire session states when this maximum is reached.</td></tr><tr><td>both</td><td>Expire session states based on time or count, whichever occurs first.</td></tr></table>				Option	Description	disable	Do not keep session states.	time	Expire session states after this many minutes.	count	Expire session states when this maximum is reached.	both	Expire session states based on time or count, whichever occurs first.				
Option	Description																	
disable	Do not keep session states.																	
time	Expire session states after this many minutes.																	
count	Expire session states when this maximum is reached.																	
both	Expire session states based on time or count, whichever occurs first.																	
ssl-dh-bits	Number of bits to use in the Diffie-Hellman exchange for RSA encryption of SSL sessions.	option	-	2048														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>768</td><td>768-bit Diffie-Hellman prime.</td></tr><tr><td>1024</td><td>1024-bit Diffie-Hellman prime.</td></tr><tr><td>1536</td><td>1536-bit Diffie-Hellman prime.</td></tr><tr><td>2048</td><td>2048-bit Diffie-Hellman prime.</td></tr><tr><td>3072</td><td>3072-bit Diffie-Hellman prime.</td></tr><tr><td>4096</td><td>4096-bit Diffie-Hellman prime.</td></tr></table>				Option	Description	768	768-bit Diffie-Hellman prime.	1024	1024-bit Diffie-Hellman prime.	1536	1536-bit Diffie-Hellman prime.	2048	2048-bit Diffie-Hellman prime.	3072	3072-bit Diffie-Hellman prime.	4096	4096-bit Diffie-Hellman prime.
Option	Description																	
768	768-bit Diffie-Hellman prime.																	
1024	1024-bit Diffie-Hellman prime.																	
1536	1536-bit Diffie-Hellman prime.																	
2048	2048-bit Diffie-Hellman prime.																	
3072	3072-bit Diffie-Hellman prime.																	
4096	4096-bit Diffie-Hellman prime.																	
ssl-hpkip	Enable/disable including HPKP header in response.	option	-	disable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Do not add a HPKP header to each HTTP response.</td></tr><tr><td>enable</td><td>Add a HPKP header to each a HTTP response.</td></tr><tr><td>report-only</td><td>Add a HPKP Report-Only header to each HTTP response.</td></tr></table>				Option	Description	disable	Do not add a HPKP header to each HTTP response.	enable	Add a HPKP header to each a HTTP response.	report-only	Add a HPKP Report-Only header to each HTTP response.						
Option	Description																	
disable	Do not add a HPKP header to each HTTP response.																	
enable	Add a HPKP header to each a HTTP response.																	
report-only	Add a HPKP Report-Only header to each HTTP response.																	

Parameter	Description	Type	Size	Default						
ssl-hpkp-age	Number of minutes the web browser should keep HPKP.	integer	Minimum value: 60 Maximum value: 157680000	5184000						
ssl-hpkp-backup	Certificate to generate backup HPKP pin from.	string	Maximum length: 79							
ssl-hpkp-include-subdomains	Indicate that HPKP header applies to all subdomains.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>HPKP header does not apply to subdomains.</td></tr><tr><td>enable</td><td>HPKP header applies to subdomains.</td></tr></table>				Option	Description	disable	HPKP header does not apply to subdomains.	enable	HPKP header applies to subdomains.
Option	Description									
disable	HPKP header does not apply to subdomains.									
enable	HPKP header applies to subdomains.									
ssl-hpkp-primary	Certificate to generate primary HPKP pin from.	string	Maximum length: 79							
ssl-hpkp-report-uri	URL to report HPKP violations to.	var-string	Maximum length: 255							
ssl-hsts	Enable/disable including HSTS header in response.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Do not add a HSTS header to each a HTTP response.</td></tr><tr><td>enable</td><td>Add a HSTS header to each HTTP response.</td></tr></table>				Option	Description	disable	Do not add a HSTS header to each a HTTP response.	enable	Add a HSTS header to each HTTP response.
Option	Description									
disable	Do not add a HSTS header to each a HTTP response.									
enable	Add a HSTS header to each HTTP response.									
ssl-hsts-age	Number of seconds the client should honor the HSTS setting.	integer	Minimum value: 60 Maximum value: 157680000	5184000						
ssl-hsts-include-subdomains	Indicate that HSTS header applies to all subdomains.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>HSTS header does not apply to subdomains.</td></tr><tr><td>enable</td><td>HSTS header applies to subdomains.</td></tr></table>				Option	Description	disable	HSTS header does not apply to subdomains.	enable	HSTS header applies to subdomains.
Option	Description									
disable	HSTS header does not apply to subdomains.									
enable	HSTS header applies to subdomains.									

Parameter	Description	Type	Size	Default												
ssl-http-location-conversion	Enable to replace HTTP with HTTPS in the reply's Location HTTP header field.	option	-	disable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable HTTP location conversion.</td></tr><tr><td><i>disable</i></td><td>Disable HTTP location conversion.</td></tr></table>	Option	Description	<i>enable</i>	Enable HTTP location conversion.	<i>disable</i>	Disable HTTP location conversion.									
Option	Description															
<i>enable</i>	Enable HTTP location conversion.															
<i>disable</i>	Disable HTTP location conversion.															
ssl-http-match-host	Enable/disable HTTP host matching for location conversion.	option	-	enable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Match HTTP host in response header.</td></tr><tr><td><i>disable</i></td><td>Do not match HTTP host.</td></tr></table>	Option	Description	<i>enable</i>	Match HTTP host in response header.	<i>disable</i>	Do not match HTTP host.									
Option	Description															
<i>enable</i>	Match HTTP host in response header.															
<i>disable</i>	Do not match HTTP host.															
ssl-max-version	Highest SSL/TLS version acceptable from a client.	option	-	tls-1.3												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ssl-3.0</i></td><td>SSL 3.0.</td></tr><tr><td><i>tls-1.0</i></td><td>TLS 1.0.</td></tr><tr><td><i>tls-1.1</i></td><td>TLS 1.1.</td></tr><tr><td><i>tls-1.2</i></td><td>TLS 1.2.</td></tr><tr><td><i>tls-1.3</i></td><td>TLS 1.3.</td></tr></table>	Option	Description	<i>ssl-3.0</i>	SSL 3.0.	<i>tls-1.0</i>	TLS 1.0.	<i>tls-1.1</i>	TLS 1.1.	<i>tls-1.2</i>	TLS 1.2.	<i>tls-1.3</i>	TLS 1.3.			
Option	Description															
<i>ssl-3.0</i>	SSL 3.0.															
<i>tls-1.0</i>	TLS 1.0.															
<i>tls-1.1</i>	TLS 1.1.															
<i>tls-1.2</i>	TLS 1.2.															
<i>tls-1.3</i>	TLS 1.3.															
ssl-min-version	Lowest SSL/TLS version acceptable from a client.	option	-	tls-1.1												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ssl-3.0</i></td><td>SSL 3.0.</td></tr><tr><td><i>tls-1.0</i></td><td>TLS 1.0.</td></tr><tr><td><i>tls-1.1</i></td><td>TLS 1.1.</td></tr><tr><td><i>tls-1.2</i></td><td>TLS 1.2.</td></tr><tr><td><i>tls-1.3</i></td><td>TLS 1.3.</td></tr></table>	Option	Description	<i>ssl-3.0</i>	SSL 3.0.	<i>tls-1.0</i>	TLS 1.0.	<i>tls-1.1</i>	TLS 1.1.	<i>tls-1.2</i>	TLS 1.2.	<i>tls-1.3</i>	TLS 1.3.			
Option	Description															
<i>ssl-3.0</i>	SSL 3.0.															
<i>tls-1.0</i>	TLS 1.0.															
<i>tls-1.1</i>	TLS 1.1.															
<i>tls-1.2</i>	TLS 1.2.															
<i>tls-1.3</i>	TLS 1.3.															
ssl-mode	Apply SSL offloading between the client and the FortiGate (half) or from the client to the FortiGate and from the FortiGate to the server (full).	option	-	half												



Parameter	Description	Type	Size	Default												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>half</i></td><td>Client to FortiGate SSL.</td></tr><tr><td><i>full</i></td><td>Client to FortiGate and FortiGate to Server SSL.</td></tr></table>	Option	Description	<i>half</i>	Client to FortiGate SSL.	<i>full</i>	Client to FortiGate and FortiGate to Server SSL.									
	Option	Description														
	<i>half</i>	Client to FortiGate SSL.														
<i>full</i>	Client to FortiGate and FortiGate to Server SSL.															
ssl-pfs	Select the cipher suites that can be used for SSL perfect forward secrecy (PFS). Applies to both client and server sessions.	option	-	require												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>require</i></td><td>Allow only Diffie-Hellman cipher-suites, so PFS is applied.</td></tr><tr><td><i>deny</i></td><td>Allow only non-Diffie-Hellman cipher-suites, so PFS is not applied.</td></tr><tr><td><i>allow</i></td><td>Allow use of any cipher suite so PFS may or may not be used depending on the cipher suite selected.</td></tr></table>	Option	Description	<i>require</i>	Allow only Diffie-Hellman cipher-suites, so PFS is applied.	<i>deny</i>	Allow only non-Diffie-Hellman cipher-suites, so PFS is not applied.	<i>allow</i>	Allow use of any cipher suite so PFS may or may not be used depending on the cipher suite selected.							
	Option	Description														
	<i>require</i>	Allow only Diffie-Hellman cipher-suites, so PFS is applied.														
	<i>deny</i>	Allow only non-Diffie-Hellman cipher-suites, so PFS is not applied.														
<i>allow</i>	Allow use of any cipher suite so PFS may or may not be used depending on the cipher suite selected.															
ssl-send-empty-frags	Enable/disable sending empty fragments to avoid CBC IV attacks (SSL 3.0 & TLS 1.0 only). May need to be disabled for compatibility with older systems.	option	-	enable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Send empty fragments.</td></tr><tr><td><i>disable</i></td><td>Do not send empty fragments.</td></tr></table>	Option	Description	<i>enable</i>	Send empty fragments.	<i>disable</i>	Do not send empty fragments.									
	Option	Description														
	<i>enable</i>	Send empty fragments.														
<i>disable</i>	Do not send empty fragments.															
ssl-server-algorithm	Permitted encryption algorithms for the server side of SSL full mode sessions according to encryption strength.	option	-	client												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>high</i></td><td>Use AES.</td></tr><tr><td><i>medium</i></td><td>Use AES, 3DES, or RC4.</td></tr><tr><td><i>low</i></td><td>Use AES, 3DES, RC4, or DES.</td></tr><tr><td><i>custom</i></td><td>Use config ssl-server-cipher-suites to select the cipher suites that are allowed.</td></tr><tr><td><i>client</i></td><td>Use the same encryption algorithms for client and server sessions.</td></tr></table>	Option	Description	<i>high</i>	Use AES.	<i>medium</i>	Use AES, 3DES, or RC4.	<i>low</i>	Use AES, 3DES, RC4, or DES.	<i>custom</i>	Use config ssl-server-cipher-suites to select the cipher suites that are allowed.	<i>client</i>	Use the same encryption algorithms for client and server sessions.			
	Option	Description														
	<i>high</i>	Use AES.														
	<i>medium</i>	Use AES, 3DES, or RC4.														
	<i>low</i>	Use AES, 3DES, RC4, or DES.														
	<i>custom</i>	Use config ssl-server-cipher-suites to select the cipher suites that are allowed.														
<i>client</i>	Use the same encryption algorithms for client and server sessions.															
ssl-server-max-version	Highest SSL/TLS version acceptable from a server. Use the client setting by default.	option	-	client												

Parameter	Description	Type	Size	Default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ssl-3.0</td><td>SSL 3.0.</td></tr><tr><td>tls-1.0</td><td>TLS 1.0.</td></tr><tr><td>tls-1.1</td><td>TLS 1.1.</td></tr><tr><td>tls-1.2</td><td>TLS 1.2.</td></tr><tr><td>tls-1.3</td><td>TLS 1.3.</td></tr><tr><td>client</td><td>Use same value as client configuration.</td></tr></table>	Option	Description	ssl-3.0	SSL 3.0.	tls-1.0	TLS 1.0.	tls-1.1	TLS 1.1.	tls-1.2	TLS 1.2.	tls-1.3	TLS 1.3.	client	Use same value as client configuration.			
	Option	Description																
	ssl-3.0	SSL 3.0.																
	tls-1.0	TLS 1.0.																
	tls-1.1	TLS 1.1.																
	tls-1.2	TLS 1.2.																
	tls-1.3	TLS 1.3.																
client	Use same value as client configuration.																	
ssl-server-min-version	Lowest SSL/TLS version acceptable from a server. Use the client setting by default.	option	-	client														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ssl-3.0</td><td>SSL 3.0.</td></tr><tr><td>tls-1.0</td><td>TLS 1.0.</td></tr><tr><td>tls-1.1</td><td>TLS 1.1.</td></tr><tr><td>tls-1.2</td><td>TLS 1.2.</td></tr><tr><td>tls-1.3</td><td>TLS 1.3.</td></tr><tr><td>client</td><td>Use same value as client configuration.</td></tr></table>	Option	Description	ssl-3.0	SSL 3.0.	tls-1.0	TLS 1.0.	tls-1.1	TLS 1.1.	tls-1.2	TLS 1.2.	tls-1.3	TLS 1.3.	client	Use same value as client configuration.			
	Option	Description																
	ssl-3.0	SSL 3.0.																
	tls-1.0	TLS 1.0.																
	tls-1.1	TLS 1.1.																
	tls-1.2	TLS 1.2.																
	tls-1.3	TLS 1.3.																
client	Use same value as client configuration.																	
ssl-server-session-state-max	Maximum number of FortiGate to Server SSL session states to keep.	integer	Minimum value: 1 Maximum value: 10000	100														
ssl-server-session-state-timeout	Number of minutes to keep FortiGate to Server SSL session state.	integer	Minimum value: 1 Maximum value: 14400	60														
ssl-server-session-state-type	How to expire SSL sessions for the segment of the SSL connection between the server and the FortiGate.	option	-	both														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Do not keep session states.</td></tr><tr><td>time</td><td>Expire session states after this many minutes.</td></tr><tr><td>count</td><td>Expire session states when this maximum is reached.</td></tr><tr><td>both</td><td>Expire session states based on time or count, whichever occurs first.</td></tr></table>	Option	Description	disable	Do not keep session states.	time	Expire session states after this many minutes.	count	Expire session states when this maximum is reached.	both	Expire session states based on time or count, whichever occurs first.							
	Option	Description																
	disable	Do not keep session states.																
	time	Expire session states after this many minutes.																
	count	Expire session states when this maximum is reached.																
both	Expire session states based on time or count, whichever occurs first.																	

Parameter	Description	Type	Size	Default
type	Configure a static NAT server load balance VIP or access proxy.	option	-	static-nat
	<b>Option</b>	<b>Description</b>		
	<i>static-nat</i>	Static NAT.		
	<i>server-load-balance</i>	Server load balance.		
	<i>access-proxy</i>	Access proxy.		
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000
weblogic-server	Enable to add an HTTP header to indicate SSL offloading for a WebLogic server.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Do not add HTTP header indicating SSL offload for WebLogic server.		
	<i>enable</i>	Add HTTP header indicating SSL offload for WebLogic server.		
websphere-server	Enable to add an HTTP header to indicate SSL offloading for a WebSphere server.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Do not add HTTP header indicating SSL offload for WebSphere server.		
	<i>enable</i>	Add HTTP header indicating SSL offload for WebSphere server.		

## config realservers

Parameter	Description	Type	Size	Default
id	Real server ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
ip	IP address of the real server.	user	Not Specified	
port	Port for communicating with the real server. Required if port forwarding is enabled.	integer	Minimum value: 1 Maximum value: 65535	0

Parameter	Description	Type	Size	Default								
status	Set the status of the real server to active so that it can accept traffic, or on standby or disabled so no traffic is sent.	option	-	active								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>active</td><td>Server status active.</td></tr><tr><td>standby</td><td>Server status standby.</td></tr><tr><td>disable</td><td>Server status disable.</td></tr></table>	Option	Description	active	Server status active.	standby	Server status standby.	disable	Server status disable.			
Option	Description											
active	Server status active.											
standby	Server status standby.											
disable	Server status disable.											
weight	Weight of the real server. If weighted load balancing is enabled, the server with the highest weight gets more connections.	integer	Minimum value: 1 Maximum value: 255	1								
holddown-interval	Time in seconds that the health check monitor continues to monitor an unresponsive server that should be active.	integer	Minimum value: 30 Maximum value: 65535	300								
healthcheck	Enable to check the responsiveness of the real server before forwarding traffic.	option	-	vip								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable per server health check.</td></tr><tr><td>enable</td><td>Enable per server health check.</td></tr><tr><td>vip</td><td>Use health check defined in VIP.</td></tr></table>	Option	Description	disable	Disable per server health check.	enable	Enable per server health check.	vip	Use health check defined in VIP.			
Option	Description											
disable	Disable per server health check.											
enable	Enable per server health check.											
vip	Use health check defined in VIP.											
http-host	HTTP server domain name in HTTP header.	string	Maximum length: 63									
max-connections	Max number of active connections that can directed to the real server. When reached, sessions are sent to other real servers.	integer	Minimum value: 0 Maximum value: 2147483647	0								
monitor <name>	Name of the health check monitor to use when polling to determine a virtual server's connectivity status. Health monitor name.	string	Maximum length: 79									
client-ip	Only clients in this IP range can connect to this real server.	user	Not Specified									

## config ssl-cipher-suites

Parameter	Description	Type	Size	Default
priority	SSL/TLS cipher suites priority.	integer	Minimum value: 0 Maximum value: 4294967295	0
cipher	Cipher suite name.	option	-	

Option	Description
<i>TLS-AES-128-GCM-SHA256</i>	Cipher suite TLS-AES-128-GCM-SHA256.
<i>TLS-AES-256-GCM-SHA384</i>	Cipher suite TLS-AES-256-GCM-SHA384.
<i>TLS-CHACHA20-POLY1305-SHA256</i>	Cipher suite TLS-CHACHA20-POLY1305-SHA256.
<i>TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256</i>	Cipher suite TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256.
<i>TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256.
<i>TLS-DHE-RSA-WITH-CHACHA20-POLY1305-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-CHACHA20-POLY1305-SHA256.
<i>TLS-DHE-RSA-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA.
<i>TLS-DHE-RSA-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA.
<i>TLS-DHE-RSA-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA256.

Parameter	Description	Type	Size	Default
	Option	Description		
	TLS-DHE-RSA-WITH-AES-128-GCM-SHA256	Cipher suite TLS-DHE-RSA-WITH-AES-128-GCM-SHA256.		
	TLS-DHE-RSA-WITH-AES-256-CBC-SHA256	Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA256.		
	TLS-DHE-RSA-WITH-AES-256-GCM-SHA384	Cipher suite TLS-DHE-RSA-WITH-AES-256-GCM-SHA384.		
	TLS-DHE-DSS-WITH-AES-128-CBC-SHA	Cipher suite TLS-DHE-DSS-WITH-AES-128-CBC-SHA.		
	TLS-DHE-DSS-WITH-AES-256-CBC-SHA	Cipher suite TLS-DHE-DSS-WITH-AES-256-CBC-SHA.		
	TLS-DHE-DSS-WITH-AES-128-CBC-SHA256	Cipher suite TLS-DHE-DSS-WITH-AES-128-CBC-SHA256.		
	TLS-DHE-DSS-WITH-AES-128-GCM-SHA256	Cipher suite TLS-DHE-DSS-WITH-AES-128-GCM-SHA256.		
	TLS-DHE-DSS-WITH-AES-256-CBC-SHA256	Cipher suite TLS-DHE-DSS-WITH-AES-256-CBC-SHA256.		
	TLS-DHE-DSS-WITH-AES-256-GCM-SHA384	Cipher suite TLS-DHE-DSS-WITH-AES-256-GCM-SHA384.		
	TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA	Cipher suite TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA.		
	TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA256	Cipher suite TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA256.		
TLS-ECDHE-RSA-WITH-AES-128-GCM-SHA256	Cipher suite TLS-ECDHE-RSA-WITH-AES-128-GCM-SHA256.			

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA.		
	<i>TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA384.		
	<i>TLS-ECDHE-RSA-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-256-GCM-SHA384.		
	<i>TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA.		
	<i>TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA256.		
	<i>TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256.		
	<i>TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA.		
	<i>TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA384.		
	<i>TLS-ECDHE-ECDSA-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-256-GCM-SHA384.		
<i>TLS-RSA-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-AES-128-CBC-SHA.			

Parameter	Description	Type	Size	Default																										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>TLS-RSA-WITH-AES-256-CBC-SHA</i></td><td>Cipher suite TLS-RSA-WITH-AES-256-CBC-SHA.</td></tr><tr><td><i>TLS-RSA-WITH-AES-128-CBC-SHA256</i></td><td>Cipher suite TLS-RSA-WITH-AES-128-CBC-SHA256.</td></tr><tr><td><i>TLS-RSA-WITH-AES-128-GCM-SHA256</i></td><td>Cipher suite TLS-RSA-WITH-AES-128-GCM-SHA256.</td></tr><tr><td><i>TLS-RSA-WITH-AES-256-CBC-SHA256</i></td><td>Cipher suite TLS-RSA-WITH-AES-256-CBC-SHA256.</td></tr><tr><td><i>TLS-RSA-WITH-AES-256-GCM-SHA384</i></td><td>Cipher suite TLS-RSA-WITH-AES-256-GCM-SHA384.</td></tr><tr><td><i>TLS-RSA-WITH-CAMELLIA-128-CBC-SHA</i></td><td>Cipher suite TLS-RSA-WITH-CAMELLIA-128-CBC-SHA.</td></tr><tr><td><i>TLS-RSA-WITH-CAMELLIA-256-CBC-SHA</i></td><td>Cipher suite TLS-RSA-WITH-CAMELLIA-256-CBC-SHA.</td></tr><tr><td><i>TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256</i></td><td>Cipher suite TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256.</td></tr><tr><td><i>TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256</i></td><td>Cipher suite TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256.</td></tr><tr><td><i>TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA</i></td><td>Cipher suite TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA.</td></tr><tr><td><i>TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA</i></td><td>Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA.</td></tr><tr><td><i>TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA</i></td><td>Cipher suite TLS-DSS-RSA-WITH-CAMELLIA-128-CBC-SHA.</td></tr></table>	Option	Description	<i>TLS-RSA-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-AES-256-CBC-SHA.	<i>TLS-RSA-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-AES-128-CBC-SHA256.	<i>TLS-RSA-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-RSA-WITH-AES-128-GCM-SHA256.	<i>TLS-RSA-WITH-AES-256-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-AES-256-CBC-SHA256.	<i>TLS-RSA-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-RSA-WITH-AES-256-GCM-SHA384.	<i>TLS-RSA-WITH-CAMELLIA-128-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-CAMELLIA-128-CBC-SHA.	<i>TLS-RSA-WITH-CAMELLIA-256-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-CAMELLIA-256-CBC-SHA.	<i>TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256.	<i>TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256.	<i>TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA.	<i>TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA.	<i>TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA</i>	Cipher suite TLS-DSS-RSA-WITH-CAMELLIA-128-CBC-SHA.			
Option	Description																													
<i>TLS-RSA-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-AES-256-CBC-SHA.																													
<i>TLS-RSA-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-AES-128-CBC-SHA256.																													
<i>TLS-RSA-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-RSA-WITH-AES-128-GCM-SHA256.																													
<i>TLS-RSA-WITH-AES-256-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-AES-256-CBC-SHA256.																													
<i>TLS-RSA-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-RSA-WITH-AES-256-GCM-SHA384.																													
<i>TLS-RSA-WITH-CAMELLIA-128-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-CAMELLIA-128-CBC-SHA.																													
<i>TLS-RSA-WITH-CAMELLIA-256-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-CAMELLIA-256-CBC-SHA.																													
<i>TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256.																													
<i>TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256.																													
<i>TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA.																													
<i>TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA.																													
<i>TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA</i>	Cipher suite TLS-DSS-RSA-WITH-CAMELLIA-128-CBC-SHA.																													



Parameter	Description	Type	Size	Default																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA</i></td><td>Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA.</td></tr><tr><td><i>TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA</i></td><td>Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA.</td></tr><tr><td><i>TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA256</i></td><td>Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA256.</td></tr><tr><td><i>TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256</i></td><td>Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256.</td></tr><tr><td><i>TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256</i></td><td>Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256.</td></tr><tr><td><i>TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256</i></td><td>Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256.</td></tr><tr><td><i>TLS-DHE-RSA-WITH-SEED-CBC-SHA</i></td><td>Cipher suite TLS-DHE-RSA-WITH-SEED-CBC-SHA.</td></tr><tr><td><i>TLS-DHE-DSS-WITH-SEED-CBC-SHA</i></td><td>Cipher suite TLS-DHE-DSS-WITH-SEED-CBC-SHA.</td></tr><tr><td><i>TLS-DHE-RSA-WITH-ARIA-128-CBC-SHA256</i></td><td>Cipher suite TLS-DHE-RSA-WITH-ARIA-128-CBC-SHA256.</td></tr><tr><td><i>TLS-DHE-RSA-WITH-ARIA-256-CBC-SHA384</i></td><td>Cipher suite TLS-DHE-RSA-WITH-ARIA-256-CBC-SHA384.</td></tr></table>	Option	Description	<i>TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA.	<i>TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA.	<i>TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA256.	<i>TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256.	<i>TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256.	<i>TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256.	<i>TLS-DHE-RSA-WITH-SEED-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-SEED-CBC-SHA.	<i>TLS-DHE-DSS-WITH-SEED-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-SEED-CBC-SHA.	<i>TLS-DHE-RSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-ARIA-128-CBC-SHA256.	<i>TLS-DHE-RSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-DHE-RSA-WITH-ARIA-256-CBC-SHA384.			
Option	Description																									
<i>TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA.																									
<i>TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA.																									
<i>TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA256.																									
<i>TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256.																									
<i>TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256.																									
<i>TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256.																									
<i>TLS-DHE-RSA-WITH-SEED-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-SEED-CBC-SHA.																									
<i>TLS-DHE-DSS-WITH-SEED-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-SEED-CBC-SHA.																									
<i>TLS-DHE-RSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-ARIA-128-CBC-SHA256.																									
<i>TLS-DHE-RSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-DHE-RSA-WITH-ARIA-256-CBC-SHA384.																									

Parameter	Description	Type	Size	Default																								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256</td><td>Cipher suite TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256.</td></tr><tr><td>TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384</td><td>Cipher suite TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384.</td></tr><tr><td>TLS-RSA-WITH-SEED-CBC-SHA</td><td>Cipher suite TLS-RSA-WITH-SEED-CBC-SHA.</td></tr><tr><td>TLS-RSA-WITH-ARIA-128-CBC-SHA256</td><td>Cipher suite TLS-RSA-WITH-ARIA-128-CBC-SHA256.</td></tr><tr><td>TLS-RSA-WITH-ARIA-256-CBC-SHA384</td><td>Cipher suite TLS-RSA-WITH-ARIA-256-CBC-SHA384.</td></tr><tr><td>TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256</td><td>Cipher suite TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256.</td></tr><tr><td>TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384</td><td>Cipher suite TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384.</td></tr><tr><td>TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC-SHA256</td><td>Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC_SHA256.</td></tr><tr><td>TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC-SHA384</td><td>Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC_SHA384.</td></tr><tr><td>TLS-ECDHE-RSA-WITH-RC4-128-SHA</td><td>Cipher suite TLS-ECDHE-RSA-WITH-RC4-128-SHA.</td></tr><tr><td>TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA</td><td>Cipher suite TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA.</td></tr></table>	Option	Description	TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256	Cipher suite TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256.	TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384	Cipher suite TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384.	TLS-RSA-WITH-SEED-CBC-SHA	Cipher suite TLS-RSA-WITH-SEED-CBC-SHA.	TLS-RSA-WITH-ARIA-128-CBC-SHA256	Cipher suite TLS-RSA-WITH-ARIA-128-CBC-SHA256.	TLS-RSA-WITH-ARIA-256-CBC-SHA384	Cipher suite TLS-RSA-WITH-ARIA-256-CBC-SHA384.	TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256	Cipher suite TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256.	TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384	Cipher suite TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384.	TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC-SHA256	Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC_SHA256.	TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC-SHA384	Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC_SHA384.	TLS-ECDHE-RSA-WITH-RC4-128-SHA	Cipher suite TLS-ECDHE-RSA-WITH-RC4-128-SHA.	TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA	Cipher suite TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA.			
Option	Description																											
TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256	Cipher suite TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256.																											
TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384	Cipher suite TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384.																											
TLS-RSA-WITH-SEED-CBC-SHA	Cipher suite TLS-RSA-WITH-SEED-CBC-SHA.																											
TLS-RSA-WITH-ARIA-128-CBC-SHA256	Cipher suite TLS-RSA-WITH-ARIA-128-CBC-SHA256.																											
TLS-RSA-WITH-ARIA-256-CBC-SHA384	Cipher suite TLS-RSA-WITH-ARIA-256-CBC-SHA384.																											
TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256	Cipher suite TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256.																											
TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384	Cipher suite TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384.																											
TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC-SHA256	Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC_SHA256.																											
TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC-SHA384	Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC_SHA384.																											
TLS-ECDHE-RSA-WITH-RC4-128-SHA	Cipher suite TLS-ECDHE-RSA-WITH-RC4-128-SHA.																											
TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA	Cipher suite TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA.																											

Parameter	Description	Type	Size	Default																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA</i></td><td>Cipher suite TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA.</td></tr><tr><td><i>TLS-RSA-WITH-3DES-EDE-CBC-SHA</i></td><td>Cipher suite TLS-RSA-WITH-3DES-EDE-CBC-SHA.</td></tr><tr><td><i>TLS-RSA-WITH-RC4-128-MD5</i></td><td>Cipher suite TLS-RSA-WITH-RC4-128-MD5.</td></tr><tr><td><i>TLS-RSA-WITH-RC4-128-SHA</i></td><td>Cipher suite TLS-RSA-WITH-RC4-128-SHA.</td></tr><tr><td><i>TLS-DHE-RSA-WITH-DES-CBC-SHA</i></td><td>Cipher suite TLS-DHE-RSA-WITH-DES-CBC-SHA.</td></tr><tr><td><i>TLS-DHE-DSS-WITH-DES-CBC-SHA</i></td><td>Cipher suite TLS-DHE-DSS-WITH-DES-CBC-SHA.</td></tr><tr><td><i>TLS-RSA-WITH-DES-CBC-SHA</i></td><td>Cipher suite TLS-RSA-WITH-DES-CBC-SHA.</td></tr></table>	Option	Description	<i>TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA.	<i>TLS-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-3DES-EDE-CBC-SHA.	<i>TLS-RSA-WITH-RC4-128-MD5</i>	Cipher suite TLS-RSA-WITH-RC4-128-MD5.	<i>TLS-RSA-WITH-RC4-128-SHA</i>	Cipher suite TLS-RSA-WITH-RC4-128-SHA.	<i>TLS-DHE-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-DES-CBC-SHA.	<i>TLS-DHE-DSS-WITH-DES-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-DES-CBC-SHA.	<i>TLS-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-DES-CBC-SHA.			
	Option	Description																		
	<i>TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA.																		
	<i>TLS-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-3DES-EDE-CBC-SHA.																		
	<i>TLS-RSA-WITH-RC4-128-MD5</i>	Cipher suite TLS-RSA-WITH-RC4-128-MD5.																		
	<i>TLS-RSA-WITH-RC4-128-SHA</i>	Cipher suite TLS-RSA-WITH-RC4-128-SHA.																		
	<i>TLS-DHE-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-DES-CBC-SHA.																		
	<i>TLS-DHE-DSS-WITH-DES-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-DES-CBC-SHA.																		
<i>TLS-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-DES-CBC-SHA.																			
versions	SSL/TLS versions that the cipher suite can be used with.	option	-	ssl-3.0 tls-1.0 tls-1.1 tls-1.2 tls-1.3																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ssl-3.0</i></td><td>SSL 3.0.</td></tr><tr><td><i>tls-1.0</i></td><td>TLS 1.0.</td></tr><tr><td><i>tls-1.1</i></td><td>TLS 1.1.</td></tr><tr><td><i>tls-1.2</i></td><td>TLS 1.2.</td></tr><tr><td><i>tls-1.3</i></td><td>TLS 1.3.</td></tr></table>	Option	Description	<i>ssl-3.0</i>	SSL 3.0.	<i>tls-1.0</i>	TLS 1.0.	<i>tls-1.1</i>	TLS 1.1.	<i>tls-1.2</i>	TLS 1.2.	<i>tls-1.3</i>	TLS 1.3.							
	Option	Description																		
	<i>ssl-3.0</i>	SSL 3.0.																		
	<i>tls-1.0</i>	TLS 1.0.																		
	<i>tls-1.1</i>	TLS 1.1.																		
	<i>tls-1.2</i>	TLS 1.2.																		
<i>tls-1.3</i>	TLS 1.3.																			

## config ssl-server-cipher-suites

Parameter	Description	Type	Size	Default
priority	SSL/TLS cipher suites priority.	integer	Minimum value: 0 Maximum value: 4294967295	0
cipher	Cipher suite name.	option	-	

Option	Description
<i>TLS-AES-128-GCM-SHA256</i>	Cipher suite TLS-AES-128-GCM-SHA256.
<i>TLS-AES-256-GCM-SHA384</i>	Cipher suite TLS-AES-256-GCM-SHA384.
<i>TLS-CHACHA20-POLY1305-SHA256</i>	Cipher suite TLS-CHACHA20-POLY1305-SHA256.
<i>TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256</i>	Cipher suite TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256.
<i>TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256.
<i>TLS-DHE-RSA-WITH-CHACHA20-POLY1305-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-CHACHA20-POLY1305-SHA256.
<i>TLS-DHE-RSA-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA.
<i>TLS-DHE-RSA-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA.
<i>TLS-DHE-RSA-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-AES-128-CBC-SHA256.

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>TLS-DHE-RSA-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-AES-128-GCM-SHA256.		
	<i>TLS-DHE-RSA-WITH-AES-256-CBC-SHA256</i>	Cipher suite TLS-DHE-RSA-WITH-AES-256-CBC-SHA256.		
	<i>TLS-DHE-RSA-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-DHE-RSA-WITH-AES-256-GCM-SHA384.		
	<i>TLS-DHE-DSS-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-AES-128-CBC-SHA.		
	<i>TLS-DHE-DSS-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-AES-256-CBC-SHA.		
	<i>TLS-DHE-DSS-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-AES-128-CBC-SHA256.		
	<i>TLS-DHE-DSS-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-AES-128-GCM-SHA256.		
	<i>TLS-DHE-DSS-WITH-AES-256-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-AES-256-CBC-SHA256.		
	<i>TLS-DHE-DSS-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-DHE-DSS-WITH-AES-256-GCM-SHA384.		
	<i>TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA.		
	<i>TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-128-CBC-SHA256.		
	<i>TLS-ECDHE-RSA-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-128-GCM-SHA256.		

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA.		
	<i>TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-256-CBC-SHA384.		
	<i>TLS-ECDHE-RSA-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-ECDHE-RSA-WITH-AES-256-GCM-SHA384.		
	<i>TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA.		
	<i>TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-CBC-SHA256.		
	<i>TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256.		
	<i>TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA.		
	<i>TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-256-CBC-SHA384.		
	<i>TLS-ECDHE-ECDSA-WITH-AES-256-GCM-SHA384</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-AES-256-GCM-SHA384.		
<i>TLS-RSA-WITH-AES-128-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-AES-128-CBC-SHA.			

Parameter	Description	Type	Size	Default																										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>TLS-RSA-WITH-AES-256-CBC-SHA</td><td>Cipher suite TLS-RSA-WITH-AES-256-CBC-SHA.</td></tr><tr><td>TLS-RSA-WITH-AES-128-CBC-SHA256</td><td>Cipher suite TLS-RSA-WITH-AES-128-CBC-SHA256.</td></tr><tr><td>TLS-RSA-WITH-AES-128-GCM-SHA256</td><td>Cipher suite TLS-RSA-WITH-AES-128-GCM-SHA256.</td></tr><tr><td>TLS-RSA-WITH-AES-256-CBC-SHA256</td><td>Cipher suite TLS-RSA-WITH-AES-256-CBC-SHA256.</td></tr><tr><td>TLS-RSA-WITH-AES-256-GCM-SHA384</td><td>Cipher suite TLS-RSA-WITH-AES-256-GCM-SHA384.</td></tr><tr><td>TLS-RSA-WITH-CAMELLIA-128-CBC-SHA</td><td>Cipher suite TLS-RSA-WITH-CAMELLIA-128-CBC-SHA.</td></tr><tr><td>TLS-RSA-WITH-CAMELLIA-256-CBC-SHA</td><td>Cipher suite TLS-RSA-WITH-CAMELLIA-256-CBC-SHA.</td></tr><tr><td>TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256</td><td>Cipher suite TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256.</td></tr><tr><td>TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256</td><td>Cipher suite TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256.</td></tr><tr><td>TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA</td><td>Cipher suite TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA.</td></tr><tr><td>TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA</td><td>Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA.</td></tr><tr><td>TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA</td><td>Cipher suite TLS-DSS-RSA-WITH-CAMELLIA-128-CBC-SHA.</td></tr></table>	Option	Description	TLS-RSA-WITH-AES-256-CBC-SHA	Cipher suite TLS-RSA-WITH-AES-256-CBC-SHA.	TLS-RSA-WITH-AES-128-CBC-SHA256	Cipher suite TLS-RSA-WITH-AES-128-CBC-SHA256.	TLS-RSA-WITH-AES-128-GCM-SHA256	Cipher suite TLS-RSA-WITH-AES-128-GCM-SHA256.	TLS-RSA-WITH-AES-256-CBC-SHA256	Cipher suite TLS-RSA-WITH-AES-256-CBC-SHA256.	TLS-RSA-WITH-AES-256-GCM-SHA384	Cipher suite TLS-RSA-WITH-AES-256-GCM-SHA384.	TLS-RSA-WITH-CAMELLIA-128-CBC-SHA	Cipher suite TLS-RSA-WITH-CAMELLIA-128-CBC-SHA.	TLS-RSA-WITH-CAMELLIA-256-CBC-SHA	Cipher suite TLS-RSA-WITH-CAMELLIA-256-CBC-SHA.	TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256	Cipher suite TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256.	TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256	Cipher suite TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256.	TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA	Cipher suite TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA.	TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA.	TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA	Cipher suite TLS-DSS-RSA-WITH-CAMELLIA-128-CBC-SHA.			
Option	Description																													
TLS-RSA-WITH-AES-256-CBC-SHA	Cipher suite TLS-RSA-WITH-AES-256-CBC-SHA.																													
TLS-RSA-WITH-AES-128-CBC-SHA256	Cipher suite TLS-RSA-WITH-AES-128-CBC-SHA256.																													
TLS-RSA-WITH-AES-128-GCM-SHA256	Cipher suite TLS-RSA-WITH-AES-128-GCM-SHA256.																													
TLS-RSA-WITH-AES-256-CBC-SHA256	Cipher suite TLS-RSA-WITH-AES-256-CBC-SHA256.																													
TLS-RSA-WITH-AES-256-GCM-SHA384	Cipher suite TLS-RSA-WITH-AES-256-GCM-SHA384.																													
TLS-RSA-WITH-CAMELLIA-128-CBC-SHA	Cipher suite TLS-RSA-WITH-CAMELLIA-128-CBC-SHA.																													
TLS-RSA-WITH-CAMELLIA-256-CBC-SHA	Cipher suite TLS-RSA-WITH-CAMELLIA-256-CBC-SHA.																													
TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256	Cipher suite TLS-RSA-WITH-CAMELLIA-128-CBC-SHA256.																													
TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256	Cipher suite TLS-RSA-WITH-CAMELLIA-256-CBC-SHA256.																													
TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA	Cipher suite TLS-DHE-RSA-WITH-3DES-EDE-CBC-SHA.																													
TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA.																													
TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA	Cipher suite TLS-DSS-RSA-WITH-CAMELLIA-128-CBC-SHA.																													

Parameter	Description	Type	Size	Default
	Option	Description		
	TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA.		
	TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA.		
	TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA256	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA256.		
	TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-128-CBC-SHA256.		
	TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256	Cipher suite TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA256.		
	TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256	Cipher suite TLS-DHE-DSS-WITH-CAMELLIA-256-CBC-SHA256.		
	TLS-DHE-RSA-WITH-SEED-CBC-SHA	Cipher suite TLS-DHE-RSA-WITH-SEED-CBC-SHA.		
	TLS-DHE-DSS-WITH-SEED-CBC-SHA	Cipher suite TLS-DHE-DSS-WITH-SEED-CBC-SHA.		
	TLS-DHE-RSA-WITH-ARIA-128-CBC-SHA256	Cipher suite TLS-DHE-RSA-WITH-ARIA-128-CBC-SHA256.		
TLS-DHE-RSA-WITH-ARIA-256-CBC-SHA384	Cipher suite TLS-DHE-RSA-WITH-ARIA-256-CBC-SHA384.			



Parameter	Description	Type	Size	Default																								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256</i></td><td>Cipher suite TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256.</td></tr><tr><td><i>TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384</i></td><td>Cipher suite TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384.</td></tr><tr><td><i>TLS-RSA-WITH-SEED-CBC-SHA</i></td><td>Cipher suite TLS-RSA-WITH-SEED-CBC-SHA.</td></tr><tr><td><i>TLS-RSA-WITH-ARIA-128-CBC-SHA256</i></td><td>Cipher suite TLS-RSA-WITH-ARIA-128-CBC-SHA256.</td></tr><tr><td><i>TLS-RSA-WITH-ARIA-256-CBC-SHA384</i></td><td>Cipher suite TLS-RSA-WITH-ARIA-256-CBC-SHA384.</td></tr><tr><td><i>TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256</i></td><td>Cipher suite TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256.</td></tr><tr><td><i>TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384</i></td><td>Cipher suite TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384.</td></tr><tr><td><i>TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC-SHA256</i></td><td>Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC_SHA256.</td></tr><tr><td><i>TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC-SHA384</i></td><td>Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC_SHA384.</td></tr><tr><td><i>TLS-ECDHE-RSA-WITH-RC4-128-SHA</i></td><td>Cipher suite TLS-ECDHE-RSA-WITH-RC4-128-SHA.</td></tr><tr><td><i>TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA</i></td><td>Cipher suite TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA.</td></tr></table>	Option	Description	<i>TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256.	<i>TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384.	<i>TLS-RSA-WITH-SEED-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-SEED-CBC-SHA.	<i>TLS-RSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-ARIA-128-CBC-SHA256.	<i>TLS-RSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-RSA-WITH-ARIA-256-CBC-SHA384.	<i>TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256.	<i>TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384.	<i>TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC_SHA256.	<i>TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC_SHA384.	<i>TLS-ECDHE-RSA-WITH-RC4-128-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-RC4-128-SHA.	<i>TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA.			
Option	Description																											
<i>TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-DHE-DSS-WITH-ARIA-128-CBC-SHA256.																											
<i>TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-DHE-DSS-WITH-ARIA-256-CBC-SHA384.																											
<i>TLS-RSA-WITH-SEED-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-SEED-CBC-SHA.																											
<i>TLS-RSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-RSA-WITH-ARIA-128-CBC-SHA256.																											
<i>TLS-RSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-RSA-WITH-ARIA-256-CBC-SHA384.																											
<i>TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-RSA-WITH-ARIA-128-CBC-SHA256.																											
<i>TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-RSA-WITH-ARIA-256-CBC-SHA384.																											
<i>TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC-SHA256</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-128-CBC_SHA256.																											
<i>TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC-SHA384</i>	Cipher suite TLS-ECDHE-ECDSA-WITH-ARIA-256-CBC_SHA384.																											
<i>TLS-ECDHE-RSA-WITH-RC4-128-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-RC4-128-SHA.																											
<i>TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-ECDHE-RSA-WITH-3DES-EDE-CBC-SHA.																											

Parameter	Description	Type	Size	Default																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA</i></td><td>Cipher suite TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA.</td></tr><tr><td><i>TLS-RSA-WITH-3DES-EDE-CBC-SHA</i></td><td>Cipher suite TLS-RSA-WITH-3DES-EDE-CBC-SHA.</td></tr><tr><td><i>TLS-RSA-WITH-RC4-128-MD5</i></td><td>Cipher suite TLS-RSA-WITH-RC4-128-MD5.</td></tr><tr><td><i>TLS-RSA-WITH-RC4-128-SHA</i></td><td>Cipher suite TLS-RSA-WITH-RC4-128-SHA.</td></tr><tr><td><i>TLS-DHE-RSA-WITH-DES-CBC-SHA</i></td><td>Cipher suite TLS-DHE-RSA-WITH-DES-CBC-SHA.</td></tr><tr><td><i>TLS-DHE-DSS-WITH-DES-CBC-SHA</i></td><td>Cipher suite TLS-DHE-DSS-WITH-DES-CBC-SHA.</td></tr><tr><td><i>TLS-RSA-WITH-DES-CBC-SHA</i></td><td>Cipher suite TLS-RSA-WITH-DES-CBC-SHA.</td></tr></table>	Option	Description	<i>TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA.	<i>TLS-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-3DES-EDE-CBC-SHA.	<i>TLS-RSA-WITH-RC4-128-MD5</i>	Cipher suite TLS-RSA-WITH-RC4-128-MD5.	<i>TLS-RSA-WITH-RC4-128-SHA</i>	Cipher suite TLS-RSA-WITH-RC4-128-SHA.	<i>TLS-DHE-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-DES-CBC-SHA.	<i>TLS-DHE-DSS-WITH-DES-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-DES-CBC-SHA.	<i>TLS-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-DES-CBC-SHA.			
	Option	Description																		
	<i>TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-3DES-EDE-CBC-SHA.																		
	<i>TLS-RSA-WITH-3DES-EDE-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-3DES-EDE-CBC-SHA.																		
	<i>TLS-RSA-WITH-RC4-128-MD5</i>	Cipher suite TLS-RSA-WITH-RC4-128-MD5.																		
	<i>TLS-RSA-WITH-RC4-128-SHA</i>	Cipher suite TLS-RSA-WITH-RC4-128-SHA.																		
	<i>TLS-DHE-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-DHE-RSA-WITH-DES-CBC-SHA.																		
	<i>TLS-DHE-DSS-WITH-DES-CBC-SHA</i>	Cipher suite TLS-DHE-DSS-WITH-DES-CBC-SHA.																		
<i>TLS-RSA-WITH-DES-CBC-SHA</i>	Cipher suite TLS-RSA-WITH-DES-CBC-SHA.																			
versions	SSL/TLS versions that the cipher suite can be used with.	option	-	ssl-3.0 tls-1.0 tls-1.1 tls-1.2 tls-1.3																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ssl-3.0</i></td><td>SSL 3.0.</td></tr><tr><td><i>tls-1.0</i></td><td>TLS 1.0.</td></tr><tr><td><i>tls-1.1</i></td><td>TLS 1.1.</td></tr><tr><td><i>tls-1.2</i></td><td>TLS 1.2.</td></tr><tr><td><i>tls-1.3</i></td><td>TLS 1.3.</td></tr></table>	Option	Description	<i>ssl-3.0</i>	SSL 3.0.	<i>tls-1.0</i>	TLS 1.0.	<i>tls-1.1</i>	TLS 1.1.	<i>tls-1.2</i>	TLS 1.2.	<i>tls-1.3</i>	TLS 1.3.							
	Option	Description																		
	<i>ssl-3.0</i>	SSL 3.0.																		
	<i>tls-1.0</i>	TLS 1.0.																		
	<i>tls-1.1</i>	TLS 1.1.																		
	<i>tls-1.2</i>	TLS 1.2.																		
<i>tls-1.3</i>	TLS 1.3.																			

## config firewall vipgrp

Configure IPv4 virtual IP groups.

```
config firewall vipgrp
  Description: Configure IPv4 virtual IP groups.
  edit <name>
    set color {integer}
    set comments {var-string}
```

```

        set interface {string}
        set member <name1>, <name2>, ...
        set uuid {uuid}
    next
end

```

## config firewall vipgrp

Parameter	Description	Type	Size	Default
color	Integer value to determine the color of the icon in the GUI.	integer	Minimum value: 0 Maximum value: 32	0
comments	Comment.	var-string	Maximum length: 255	
interface	Interface.	string	Maximum length: 35	
member <name>	Member VIP objects of the group (Separate multiple objects with a space). VIP name.	string	Maximum length: 79	
name	VIP group name.	string	Maximum length: 79	
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000

## config firewall vipgrp6

Configure IPv6 virtual IP groups.

```

config firewall vipgrp6
    Description: Configure IPv6 virtual IP groups.
    edit <name>
        set color {integer}
        set comments {var-string}
        set member <name1>, <name2>, ...
        set uuid {uuid}
    next
end

```

## config firewall vipgrp6

Parameter	Description	Type	Size	Default
color	Integer value to determine the color of the icon in the GUI.	integer	Minimum value: 0 Maximum value: 32	0
comments	Comment.	var-string	Maximum length: 255	
member <name>	Member VIP objects of the group (Separate multiple objects with a space). IPv6 VIP name.	string	Maximum length: 79	
name	IPv6 VIP group name.	string	Maximum length: 79	
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000

## config firewall wildcard-fqdn custom

Config global/VDOM Wildcard FQDN address.

```
config firewall wildcard-fqdn custom
    Description: Config global/VDOM Wildcard FQDN address.
    edit <name>
        set color {integer}
        set comment {var-string}
        set uuid {uuid}
        set wildcard-fqdn {string}
    next
end
```

## config firewall wildcard-fqdn custom

Parameter	Description	Type	Size	Default
color	GUI icon color.	integer	Minimum value: 0 Maximum value: 32	0
comment	Comment.	var-string	Maximum length: 255	
name	Address name.	string	Maximum length: 79	

Parameter	Description	Type	Size	Default
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000
wildcard-fqdn	Wildcard FQDN.	string	Maximum length: 255	

## config firewall wildcard-fqdn group

Config global Wildcard FQDN address groups.

```
config firewall wildcard-fqdn group
    Description: Config global Wildcard FQDN address groups.
    edit <name>
        set color {integer}
        set comment {var-string}
        set member <name1>, <name2>, ...
        set uuid {uuid}
    next
end
```

## config firewall wildcard-fqdn group

Parameter	Description	Type	Size	Default
color	GUI icon color.	integer	Minimum value: 0 Maximum value: 32	0
comment	Comment.	var-string	Maximum length: 255	
member <name>	Address group members. Address name.	string	Maximum length: 79	
name	Address group name.	string	Maximum length: 79	
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000

## ftp-proxy

This section includes syntax for the following commands:

- [config ftp-proxy explicit on page 514](#)

### config ftp-proxy explicit

Configure explicit FTP proxy settings.

```
config ftp-proxy explicit
    Description: Configure explicit FTP proxy settings.
    set incoming-ip {ipv4-address-any}
    set incoming-port {user}
    set outgoing-ip {ipv4-address-any}
    set sec-default-action [accept|deny]
    set ssl [enable|disable]
    set ssl-algorithm [high|medium|...]
    set ssl-cert {string}
    set ssl-dh-bits [768|1024|...]
    set status [enable|disable]
end
```

### config ftp-proxy explicit

Parameter	Description	Type	Size	Default
incoming-ip	Accept incoming FTP requests from this IP address. An interface must have this IP address.	ipv4-address-any	Not Specified	0.0.0.0
incoming-port	Accept incoming FTP requests on one or more ports.	user	Not Specified	
outgoing-ip	Outgoing FTP requests will leave from this IP address. An interface must have this IP address.	ipv4-address-any	Not Specified	
sec-default-action	Accept or deny explicit FTP proxy sessions when no FTP proxy firewall policy exists.	option	-	deny
	Option	Description		
	accept	Accept requests. All explicit FTP proxy traffic is accepted whether there is an explicit FTP proxy policy or not		
	deny	Deny requests unless there is a matching explicit FTP proxy policy.		
ssl	Enable/disable the explicit FTPS proxy.	option	-	disable

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable the explicit FTPS proxy.		
	<i>disable</i>	Disable the explicit FTPS proxy.		
ssl-algorithm	Relative strength of encryption algorithms accepted in negotiation.	option	-	high
	<b>Option</b>	<b>Description</b>		
	<i>high</i>	High encryption. Allow only AES and ChaCha		
	<i>medium</i>	Medium encryption. Allow AES, ChaCha, 3DES, and RC4.		
	<i>low</i>	Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.		
ssl-cert	Name of certificate for SSL connections to this server.	string	Maximum length: 35	Fortinet_CA_SSL
ssl-dh-bits	Bit-size of Diffie-Hellman.	option	-	2048
	<b>Option</b>	<b>Description</b>		
	<i>768</i>	768-bit Diffie-Hellman prime.		
	<i>1024</i>	1024-bit Diffie-Hellman prime.		
	<i>1536</i>	1536-bit Diffie-Hellman prime.		
	<i>2048</i>	2048-bit Diffie-Hellman prime.		
status	Enable/disable the explicit FTP proxy.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable the explicit FTP proxy.		
	<i>disable</i>	Disable the explicit FTP proxy.		

## gtp

This section includes syntax for the following commands:

- [config gtp apn-shaper on page 516](#)
- [config gtp apn on page 518](#)
- [config gtp apngrp on page 519](#)
- [config gtp ie-allow-list on page 520](#)
- [config gtp message-filter-v0v1 on page 521](#)
- [config gtp message-filter-v2 on page 529](#)
- [config gtp rat-timeout-profile on page 534](#)
- [config gtp tunnel-limit on page 536](#)

### config gtp apn-shaper



This command is available for model(s): FortiGate 2600F, FortiGate 3000F, FortiGate 3001F, FortiGate 3400E.

It is not available for: FortiGate 1000D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2601F, FortiGate 3000D, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

Global per-APN shaper.

```
config gtp apn-shaper
  Description: Global per-APN shaper.
  edit <id>
    set action [drop|reject]
    set apn <name1>, <name2>, ...
```



```

        set back-off-time {integer}
        set rate-limit {integer}
    next
end

```

## config gtp apn-shaper

Parameter	Description	Type	Size	Default
action	Action.	option	-	drop
	<b>Option</b>	<b>Description</b>		
	<i>drop</i>	Drop packet if exceeding rate limit.		
	<i>reject</i>	Reject packet if exceeding rate limit.		
apn <name>	APN names to match. Leave empty to match ANY. APN name.	string	Maximum length: 79	
back-off-time	Back off time in seconds.	integer	Minimum value: 10 Maximum value: 360	0
id	Shaper ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
rate-limit	Rate limit in packets/s.	integer	Minimum value: 0 Maximum value: 1000000	0

## config gtp apn



This command is available for model(s): FortiGate 2600F, FortiGate 3000F, FortiGate 3001F, FortiGate 3400E.

It is not available for: FortiGate 1000D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2601F, FortiGate 3000D, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

Configure APN for GTP.

```
config gtp apn
    Description: Configure APN for GTP.
    edit <name>
        set apn {string}
    next
end
```

## config gtp apn

Parameter	Description	Type	Size	Default
apn	APN value.	string	Maximum length: 102	
name	APN name.	string	Maximum length: 63	

## config gtp apngrp



This command is available for model(s): FortiGate 2600F, FortiGate 3000F, FortiGate 3001F, FortiGate 3400E.

It is not available for: FortiGate 1000D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2601F, FortiGate 3000D, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

Configure APN groups for GTP.

```
config gtp apngrp
    Description: Configure APN groups for GTP.
    edit <name>
        set member <name1>, <name2>, ...
    next
end
```

## config gtp apngrp

Parameter	Description	Type	Size	Default
member <name>	APN group member. APN name.	string	Maximum length: 79	
name	GTP APN group name.	string	Maximum length: 63	

## config gtp ie-allow-list



This command is available for model(s): FortiGate 2600F, FortiGate 3000F, FortiGate 3001F, FortiGate 3400E.

It is not available for: FortiGate 1000D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2601F, FortiGate 3000D, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

IE allow list.

```
config gtp ie-allow-list
  Description: IE allow list.
  edit <name>
    config entries
      Description: Entries of allow list for unknown or out-of-state IEs.
      edit <id>
        set message {integer}
        set ie {integer}
      next
    end
  next
end
```

## config gtp ie-allow-list

Parameter	Description	Type	Size	Default
name	IE allow list name.	string	Maximum length: 63	

## config entries

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
message	Message ID.	integer	Minimum value: 1 Maximum value: 255	0
ie	IE ID.	integer	Minimum value: 1 Maximum value: 255	0

## config gtp message-filter-v0v1



This command is available for model(s): FortiGate 2600F, FortiGate 3000F, FortiGate 3001F, FortiGate 3400E.

It is not available for: FortiGate 1000D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2601F, FortiGate 3000D, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

Message filter for GTPv0/v1 messages.

```
config gtp message-filter-v0v1
  Description: Message filter for GTPv0/v1 messages.
  edit <name>
```

```

set create-mbms [allow|deny]
set create-pdp [allow|deny]
set data-record [allow|deny]
set delete-aa-pdp [allow|deny]
set delete-mbms [allow|deny]
set delete-pdp [allow|deny]
set echo [allow|deny]
set end-marker [allow|deny]
set error-indication [allow|deny]
set failure-report [allow|deny]
set fwd-relocation [allow|deny]
set fwd-srns-context [allow|deny]
set gtp-pdu [allow|deny]
set identification [allow|deny]
set mbms-de-registration [allow|deny]
set mbms-notification [allow|deny]
set mbms-registration [allow|deny]
set mbms-session-start [allow|deny]
set mbms-session-stop [allow|deny]
set mbms-session-update [allow|deny]
set ms-info-change-notif [allow|deny]
set node-alive [allow|deny]
set note-ms-present [allow|deny]
set pdu-notification [allow|deny]
set ran-info [allow|deny]
set redirection [allow|deny]
set relocation-cancel [allow|deny]
set send-route [allow|deny]
set sgsn-context [allow|deny]
set support-extension [allow|deny]
set unknown-message [allow|deny]
set unknown-message-white-list <id1>, <id2>, ...
set update-mbms [allow|deny]
set update-pdp [allow|deny]
set v0-create-aa-pdp--v1-init-pdp-ctx [allow|deny]
set version-not-support [allow|deny]

```

next

end

## config gtp message-filter-v0v1

Parameter	Description	Type	Size	Default
create-mbms	GTPv1 create MBMS context (req 100, resp 101).	option	-	allow
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow message.		
	<i>deny</i>	Deny message.		
create-pdp	Create PDP context (req 16, resp 17).	option	-	allow

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow message.		
	<i>deny</i>	Deny message.		
data-record	Data record transfer (req 240, resp 241).	option	-	allow
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow message.		
	<i>deny</i>	Deny message.		
delete-aa-pdp	GTPv0 delete AA PDP context (req 24, resp 25).	option	-	allow
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow message.		
	<i>deny</i>	Deny message.		
delete-mbms	GTPv1 delete MBMS context (req 104, resp 105).	option	-	allow
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow message.		
	<i>deny</i>	Deny message.		
delete-pdp	Delete PDP context (req 20, resp 21).	option	-	allow
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow message.		
	<i>deny</i>	Deny message.		
echo	Echo (req 1, resp 2).	option	-	allow
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow message.		
	<i>deny</i>	Deny message.		
end-marker	GTPv1 End marker (254).	option	-	allow
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow message.		
	<i>deny</i>	Deny message.		
error-indication	Error indication (26).	option	-	allow

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow message.		
	<i>deny</i>	Deny message.		
failure-report	Failure report (req 34, resp 35).	option	-	allow
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow message.		
	<i>deny</i>	Deny message.		
fwd-relocation	GTPv1 forward relocation (req 53, resp 54, complete 55, complete ack 59).	option	-	allow
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow message.		
	<i>deny</i>	Deny message.		
fwd-srns-context	GTPv1 forward SRNS (context 58, context ack 60).	option	-	allow
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow message.		
	<i>deny</i>	Deny message.		
gtp-pdu	PDU (255).	option	-	allow
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow message.		
	<i>deny</i>	Deny message.		
identification	Identification (req 48, resp 49).	option	-	allow
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow message.		
	<i>deny</i>	Deny message.		
mbms-de-registration	GTPv1 MBMS de-registration (req 114, resp 115).	option	-	allow



Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow message.		
	<i>deny</i>	Deny message.		
mbms-notification	GTPv1 MBMS notification (req 96, resp 97, reject req 98. reject resp 99).	option	-	allow
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow message.		
	<i>deny</i>	Deny message.		
mbms-registration	GTPv1 MBMS registration (req 112, resp 113).	option	-	allow
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow message.		
	<i>deny</i>	Deny message.		
mbms-session-start	GTPv1 MBMS session start (req 116, resp 117).	option	-	allow
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow message.		
	<i>deny</i>	Deny message.		
mbms-session-stop	GTPv1 MBMS session stop (req 118, resp 119).	option	-	allow
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow message.		
	<i>deny</i>	Deny message.		
mbms-session-update	GTPv1 MBMS session update (req 120, resp 121).	option	-	allow
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow message.		
	<i>deny</i>	Deny message.		

Parameter	Description	Type	Size	Default						
ms-info-change-notif	GTPv1 MS info change notification (req 128, resp 129).	option	-	allow						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow message.</td></tr><tr><td><i>deny</i></td><td>Deny message.</td></tr></table>	Option	Description	<i>allow</i>	Allow message.	<i>deny</i>	Deny message.			
Option	Description									
<i>allow</i>	Allow message.									
<i>deny</i>	Deny message.									
name	Message filter name.	string	Maximum length: 63							
node-alive	Node alive (req 4, resp 5).	option	-	allow						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow message.</td></tr><tr><td><i>deny</i></td><td>Deny message.</td></tr></table>	Option	Description	<i>allow</i>	Allow message.	<i>deny</i>	Deny message.			
Option	Description									
<i>allow</i>	Allow message.									
<i>deny</i>	Deny message.									
note-ms-present	Note MS GPRS present (req 36, resp 37).	option	-	allow						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow message.</td></tr><tr><td><i>deny</i></td><td>Deny message.</td></tr></table>	Option	Description	<i>allow</i>	Allow message.	<i>deny</i>	Deny message.			
Option	Description									
<i>allow</i>	Allow message.									
<i>deny</i>	Deny message.									
pdu-notification	PDU notification (req 27, resp 28, reject req 29, reject resp 30).	option	-	allow						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow message.</td></tr><tr><td><i>deny</i></td><td>Deny message.</td></tr></table>	Option	Description	<i>allow</i>	Allow message.	<i>deny</i>	Deny message.			
Option	Description									
<i>allow</i>	Allow message.									
<i>deny</i>	Deny message.									
ran-info	GTPv1 RAN information relay (70).	option	-	allow						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow message.</td></tr><tr><td><i>deny</i></td><td>Deny message.</td></tr></table>	Option	Description	<i>allow</i>	Allow message.	<i>deny</i>	Deny message.			
Option	Description									
<i>allow</i>	Allow message.									
<i>deny</i>	Deny message.									
redirection	Redirection (req 6, resp 7).	option	-	allow						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow message.</td></tr><tr><td><i>deny</i></td><td>Deny message.</td></tr></table>	Option	Description	<i>allow</i>	Allow message.	<i>deny</i>	Deny message.			
Option	Description									
<i>allow</i>	Allow message.									
<i>deny</i>	Deny message.									

Parameter	Description	Type	Size	Default						
relocation-cancel	GTPv1 relocation cancel (req 56, resp 57).	option	-	allow						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow message.</td></tr><tr><td><i>deny</i></td><td>Deny message.</td></tr></table>	Option	Description	<i>allow</i>	Allow message.	<i>deny</i>	Deny message.			
Option	Description									
<i>allow</i>	Allow message.									
<i>deny</i>	Deny message.									
send-route	Send routing information for GPRS (req 32, resp 33).	option	-	allow						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow message.</td></tr><tr><td><i>deny</i></td><td>Deny message.</td></tr></table>	Option	Description	<i>allow</i>	Allow message.	<i>deny</i>	Deny message.			
Option	Description									
<i>allow</i>	Allow message.									
<i>deny</i>	Deny message.									
sgsn-context	SGSN context (req 50, resp 51, ack 52).	option	-	allow						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow message.</td></tr><tr><td><i>deny</i></td><td>Deny message.</td></tr></table>	Option	Description	<i>allow</i>	Allow message.	<i>deny</i>	Deny message.			
Option	Description									
<i>allow</i>	Allow message.									
<i>deny</i>	Deny message.									
support-extension	GTPv1 supported extension headers notify (31).	option	-	allow						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow message.</td></tr><tr><td><i>deny</i></td><td>Deny message.</td></tr></table>	Option	Description	<i>allow</i>	Allow message.	<i>deny</i>	Deny message.			
Option	Description									
<i>allow</i>	Allow message.									
<i>deny</i>	Deny message.									
unknown-message	Allow or Deny unknown messages.	option	-	allow						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow setting.</td></tr><tr><td><i>deny</i></td><td>Deny setting.</td></tr></table>	Option	Description	<i>allow</i>	Allow setting.	<i>deny</i>	Deny setting.			
Option	Description									
<i>allow</i>	Allow setting.									
<i>deny</i>	Deny setting.									
unknown-message-white-list <id>	White list (to allow) of unknown messages. Message IDs.	integer	Minimum value: 1 Maximum value: 255							
update-mbms	GTPv1 update MBMS context (req 102, resp 103).	option	-	allow						

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow message.		
	<i>deny</i>	Deny message.		
update-pdp	Update PDP context (req 18, resp 19).	option	-	allow
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow message.		
	<i>deny</i>	Deny message.		
v0-create-aa-pdp--v1-init-pdp-ctx	GTPv0 create AA PDP context (req 22, resp 23); Or GTPv1 initiate PDP context (req 22, resp 23).	option	-	allow
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow message.		
	<i>deny</i>	Deny message.		
version-not-support	Version not supported (3).	option	-	allow
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow message.		
	<i>deny</i>	Deny message.		

---

## config gtp message-filter-v2

---



This command is available for model(s): FortiGate 2600F, FortiGate 3000F, FortiGate 3001F, FortiGate 3400E.

It is not available for: FortiGate 1000D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2601F, FortiGate 3000D, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

---

Message filter for GTPv2 messages.

```
config gtp message-filter-v2
  Description: Message filter for GTPv2 messages.
  edit <name>
    set bearer-resource-cmd-fail [allow|deny]
    set change-notification [allow|deny]
    set context-req-res-ack [allow|deny]
    set create-bearer [allow|deny]
    set create-session [allow|deny]
    set delete-bearer-cmd-fail [allow|deny]
    set delete-bearer-req-resp [allow|deny]
    set delete-pdn-connection-set [allow|deny]
    set delete-session [allow|deny]
    set echo [allow|deny]
    set forward-relocation-cmp-notif-ack [allow|deny]
    set forward-relocation-req-res [allow|deny]
    set modify-bearer-cmd-fail [allow|deny]
    set modify-bearer-req-resp [allow|deny]
    set resume [allow|deny]
    set suspend [allow|deny]
    set trace-session [allow|deny]
    set unknown-message [allow|deny]
    set unknown-message-white-list <id1>, <id2>, ...
    set update-bearer [allow|deny]
    set update-pdn-connection-set [allow|deny]
    set version-not-support [allow|deny]
```

next  
end

## config gtp message-filter-v2

Parameter	Description	Type	Size	Default						
bearer-resource-cmd-fail	Bearer resource (command 68, failure indication 69).	option	-	allow						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow message.</td></tr><tr><td><i>deny</i></td><td>Deny message.</td></tr></table>	Option	Description	<i>allow</i>	Allow message.	<i>deny</i>	Deny message.			
Option	Description									
<i>allow</i>	Allow message.									
<i>deny</i>	Deny message.									
change-notification	Change notification (req 38, resp 39).	option	-	allow						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow message.</td></tr><tr><td><i>deny</i></td><td>Deny message.</td></tr></table>	Option	Description	<i>allow</i>	Allow message.	<i>deny</i>	Deny message.			
Option	Description									
<i>allow</i>	Allow message.									
<i>deny</i>	Deny message.									
context-req-res-ack	Context request/response/acknowledge (req 130, resp 131, ack 132).	option	-	allow						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow message.</td></tr><tr><td><i>deny</i></td><td>Deny message.</td></tr></table>	Option	Description	<i>allow</i>	Allow message.	<i>deny</i>	Deny message.			
Option	Description									
<i>allow</i>	Allow message.									
<i>deny</i>	Deny message.									
create-bearer	Create bearer (req 95, resp 96).	option	-	allow						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow message.</td></tr><tr><td><i>deny</i></td><td>Deny message.</td></tr></table>	Option	Description	<i>allow</i>	Allow message.	<i>deny</i>	Deny message.			
Option	Description									
<i>allow</i>	Allow message.									
<i>deny</i>	Deny message.									
create-session	Create session (req 32, resp 33).	option	-	allow						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow message.</td></tr><tr><td><i>deny</i></td><td>Deny message.</td></tr></table>	Option	Description	<i>allow</i>	Allow message.	<i>deny</i>	Deny message.			
Option	Description									
<i>allow</i>	Allow message.									
<i>deny</i>	Deny message.									
delete-bearer-cmd-fail	Delete bearer (command 66, failure indication 67).	option	-	allow						

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow message.		
	<i>deny</i>	Deny message.		
delete-bearer-req-resp	Delete bearer (req 99, resp 100).	option	-	allow
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow message.		
	<i>deny</i>	Deny message.		
delete-pdn-connection-set	Delete PDN connection set (req 101, resp 102).	option	-	allow
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow message.		
	<i>deny</i>	Deny message.		
delete-session	Delete session (req 36, resp 37).	option	-	allow
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow message.		
	<i>deny</i>	Deny message.		
echo	Echo (req 1, resp 2).	option	-	allow
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow message.		
	<i>deny</i>	Deny message.		
forward-relocation-cmp-notif-ack	Forward relocation complete notification/acknowledge (notif 135, ack 136).	option	-	allow
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow message.		
	<i>deny</i>	Deny message.		

Parameter	Description	Type	Size	Default						
forward-relocation-req-res	Forward relocation request/response (req 133, resp 134).	option	-	allow						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow message.</td></tr><tr><td><i>deny</i></td><td>Deny message.</td></tr></table>	Option	Description	<i>allow</i>	Allow message.	<i>deny</i>	Deny message.			
Option	Description									
<i>allow</i>	Allow message.									
<i>deny</i>	Deny message.									
modify-bearer-cmd-fail	Modify bearer (command 64 , failure indication 65).	option	-	allow						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow message.</td></tr><tr><td><i>deny</i></td><td>Deny message.</td></tr></table>	Option	Description	<i>allow</i>	Allow message.	<i>deny</i>	Deny message.			
Option	Description									
<i>allow</i>	Allow message.									
<i>deny</i>	Deny message.									
modify-bearer-req-resp	Modify bearer (req 34, resp 35).	option	-	allow						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow message.</td></tr><tr><td><i>deny</i></td><td>Deny message.</td></tr></table>	Option	Description	<i>allow</i>	Allow message.	<i>deny</i>	Deny message.			
Option	Description									
<i>allow</i>	Allow message.									
<i>deny</i>	Deny message.									
name	Message filter name.	string	Maximum length: 63							
resume	Resume (notify 164 , ack 165).	option	-	allow						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow message.</td></tr><tr><td><i>deny</i></td><td>Deny message.</td></tr></table>	Option	Description	<i>allow</i>	Allow message.	<i>deny</i>	Deny message.			
Option	Description									
<i>allow</i>	Allow message.									
<i>deny</i>	Deny message.									
suspend	Suspend (notify 162, ack 163).	option	-	allow						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow message.</td></tr><tr><td><i>deny</i></td><td>Deny message.</td></tr></table>	Option	Description	<i>allow</i>	Allow message.	<i>deny</i>	Deny message.			
Option	Description									
<i>allow</i>	Allow message.									
<i>deny</i>	Deny message.									
trace-session	Trace session (activation 71, deactivation 72).	option	-	allow						



Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow message.		
	<i>deny</i>	Deny message.		
unknown-message	Allow or Deny unknown messages.	option	-	allow
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow setting.		
	<i>deny</i>	Deny setting.		
unknown-message-white-list <id>	White list (to allow) of unknown messages. Message IDs.	integer	Minimum value: 1 Maximum value: 255	
update-bearer	Update bearer (req 97, resp 98).	option	-	allow
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow message.		
	<i>deny</i>	Deny message.		
update-pdn-connection-set	Update PDN connection set (req 200, resp 201).	option	-	allow
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow message.		
	<i>deny</i>	Deny message.		
version-not-support	Version not supported (3).	option	-	allow
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow message.		
	<i>deny</i>	Deny message.		

## config gtp rat-timeout-profile



This command is available for model(s): FortiGate 2600F, FortiGate 3000F, FortiGate 3001F, FortiGate 3400E.

It is not available for: FortiGate 1000D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2601F, FortiGate 3000D, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

### RAT timeout profile

```
config gtp rat-timeout-profile
  Description: RAT timeout profile
  edit <name>
    set eutran-timeout {integer}
    set gan-timeout {integer}
    set geran-timeout {integer}
    set hspa-timeout {integer}
    set ltem-timeout {integer}
    set nbiot-timeout {integer}
    set nr-timeout {integer}
    set utran-timeout {integer}
    set virtual-timeout {integer}
    set wlan-timeout {integer}
  next
end
```

## config gtp rat-timeout-profile

Parameter	Description	Type	Size	Default
eutran-timeout	Established eutran timeout in seconds.	integer	Minimum value: 0 Maximum value: 4294967295	0
gan-timeout	Established gan timeout in seconds.	integer	Minimum value: 0 Maximum value: 4294967295	0
geran-timeout	Established geran timeout in seconds.	integer	Minimum value: 0 Maximum value: 4294967295	0
hspa-timeout	Established hspa timeout in seconds.	integer	Minimum value: 0 Maximum value: 4294967295	0
Item-timeout	Established Item timeout in seconds.	integer	Minimum value: 0 Maximum value: 4294967295	0
name	RAT timeout profile name.	string	Maximum length: 63	
nbiot-timeout	Established nbiot timeout in seconds.	integer	Minimum value: 0 Maximum value: 4294967295	0
nr-timeout	Established nr timeout in seconds.	integer	Minimum value: 0 Maximum value: 4294967295	0

Parameter	Description	Type	Size	Default
utran-timeout	Established utran timeout in seconds.	integer	Minimum value: 0 Maximum value: 4294967295	0
virtual-timeout	Established virtual timeout in seconds.	integer	Minimum value: 0 Maximum value: 4294967295	0
wlan-timeout	Established wlan timeout in seconds.	integer	Minimum value: 0 Maximum value: 4294967295	0

## config gtp tunnel-limit



This command is available for model(s): FortiGate 2600F, FortiGate 3000F, FortiGate 3001F, FortiGate 3400E.

It is not available for: FortiGate 1000D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2601F, FortiGate 3000D, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

GTP tunnel limiter.

```
config gtp tunnel-limit
  Description: GTP tunnel limiter.
```

```
edit <name>
    set tunnel-limit {integer}
next
end
```

## config gtp tunnel-limit

Parameter	Description	Type	Size	Default
name	Tunnel limiter name.	string	Maximum length: 63	
tunnel-limit	Tunnel limit [1, 16000000].	integer	Minimum value: 1 Maximum value: 16000000	0

## icap

This section includes syntax for the following commands:

- [config icap profile on page 538](#)
- [config icap server on page 543](#)

### config icap profile

Configure ICAP profiles.

```
config icap profile
  Description: Configure ICAP profiles.
  edit <name>
    set chunk-encap [disable|enable]
    set extension-feature {option1}, {option2}, ...
    set icap-block-log [disable|enable]
    config icap-headers
      Description: Configure ICAP forwarded request headers.
      edit <id>
        set name {string}
        set content {string}
        set base64-encoding [disable|enable]
      next
    end
    set methods {option1}, {option2}, ...
    set preview [disable|enable]
    set preview-data-length {integer}
    set replacemsg-group {string}
    set request [disable|enable]
    set request-failure [error|bypass]
    set request-path {string}
    set request-server {string}
    set respmod-default-action [forward|bypass]
    config respmod-forward-rules
      Description: ICAP response mode forward rules.
      edit <name>
        set host {string}
        config header-group
          Description: HTTP header group.
          edit <id>
            set header-name {string}
            set header {string}
            set case-sensitivity [disable|enable]
          next
        end
        set action [forward|bypass]
        set http-resp-status-code <code1>, <code2>, ...
      next
    end
  set response [disable|enable]
```

```

set response-failure [error|bypass]
set response-path {string}
set response-req-hdr [disable|enable]
set response-server {string}
set scan-progress-interval {integer}
set streaming-content-bypass [disable|enable]
next
end

```

## config icap profile

Parameter	Description	Type	Size	Default								
chunk-encap	Enable/disable chunked encapsulation.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Do not encapsulate chunked data.</td></tr><tr><td><i>enable</i></td><td>Encapsulate chunked data into a new chunk.</td></tr></table>	Option	Description	<i>disable</i>	Do not encapsulate chunked data.	<i>enable</i>	Encapsulate chunked data into a new chunk.					
Option	Description											
<i>disable</i>	Do not encapsulate chunked data.											
<i>enable</i>	Encapsulate chunked data into a new chunk.											
extension-feature	Enable/disable ICAP extension features.	option	-									
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>scan-progress</i></td><td>Support X-Scan-Progress-Interval ICAP header.</td></tr></table>	Option	Description	<i>scan-progress</i>	Support X-Scan-Progress-Interval ICAP header.							
Option	Description											
<i>scan-progress</i>	Support X-Scan-Progress-Interval ICAP header.											
icap-block-log	Enable/disable UTM log when infection found.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable UTM log when infection found.</td></tr><tr><td><i>enable</i></td><td>Enable UTM log when infection found.</td></tr></table>	Option	Description	<i>disable</i>	Disable UTM log when infection found.	<i>enable</i>	Enable UTM log when infection found.					
Option	Description											
<i>disable</i>	Disable UTM log when infection found.											
<i>enable</i>	Enable UTM log when infection found.											
methods	The allowed HTTP methods that will be sent to ICAP server for further processing.	option	-	delete get head options post put trace other								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>delete</i></td><td>Forward HTTP request or response with DELETE method to ICAP server for further processing.</td></tr><tr><td><i>get</i></td><td>Forward HTTP request or response with GET method to ICAP server for further processing.</td></tr><tr><td><i>head</i></td><td>Forward HTTP request or response with HEAD method to ICAP server for further processing.</td></tr></table>	Option	Description	<i>delete</i>	Forward HTTP request or response with DELETE method to ICAP server for further processing.	<i>get</i>	Forward HTTP request or response with GET method to ICAP server for further processing.	<i>head</i>	Forward HTTP request or response with HEAD method to ICAP server for further processing.			
Option	Description											
<i>delete</i>	Forward HTTP request or response with DELETE method to ICAP server for further processing.											
<i>get</i>	Forward HTTP request or response with GET method to ICAP server for further processing.											
<i>head</i>	Forward HTTP request or response with HEAD method to ICAP server for further processing.											

Parameter	Description	Type	Size	Default												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>options</i></td><td>Forward HTTP request or response with OPTIONS method to ICAP server for further processing.</td></tr><tr><td><i>post</i></td><td>Forward HTTP request or response with POST method to ICAP server for further processing.</td></tr><tr><td><i>put</i></td><td>Forward HTTP request or response with PUT method to ICAP server for further processing.</td></tr><tr><td><i>trace</i></td><td>Forward HTTP request or response with TRACE method to ICAP server for further processing.</td></tr><tr><td><i>other</i></td><td>Forward HTTP request or response with All other methods to ICAP server for further processing.</td></tr></table>	Option	Description	<i>options</i>	Forward HTTP request or response with OPTIONS method to ICAP server for further processing.	<i>post</i>	Forward HTTP request or response with POST method to ICAP server for further processing.	<i>put</i>	Forward HTTP request or response with PUT method to ICAP server for further processing.	<i>trace</i>	Forward HTTP request or response with TRACE method to ICAP server for further processing.	<i>other</i>	Forward HTTP request or response with All other methods to ICAP server for further processing.			
	Option	Description														
	<i>options</i>	Forward HTTP request or response with OPTIONS method to ICAP server for further processing.														
	<i>post</i>	Forward HTTP request or response with POST method to ICAP server for further processing.														
	<i>put</i>	Forward HTTP request or response with PUT method to ICAP server for further processing.														
	<i>trace</i>	Forward HTTP request or response with TRACE method to ICAP server for further processing.														
<i>other</i>	Forward HTTP request or response with All other methods to ICAP server for further processing.															
name	ICAP profile name.	string	Maximum length: 35													
preview	Enable/disable preview of data to ICAP server.	option	-	disable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable preview of data to ICAP server.</td></tr><tr><td><i>enable</i></td><td>Enable preview of data to ICAP server.</td></tr></table>	Option	Description	<i>disable</i>	Disable preview of data to ICAP server.	<i>enable</i>	Enable preview of data to ICAP server.									
	Option	Description														
	<i>disable</i>	Disable preview of data to ICAP server.														
<i>enable</i>	Enable preview of data to ICAP server.															
preview-data-length	Preview data length to be sent to ICAP server.	integer	Minimum value: 0 Maximum value: 4096	0												
replacemsg-group	Replacement message group.	string	Maximum length: 35													
request	Enable/disable whether an HTTP request is passed to an ICAP server.	option	-	disable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable HTTP request passing to ICAP server.</td></tr><tr><td><i>enable</i></td><td>Enable HTTP request passing to ICAP server.</td></tr></table>	Option	Description	<i>disable</i>	Disable HTTP request passing to ICAP server.	<i>enable</i>	Enable HTTP request passing to ICAP server.									
	Option	Description														
	<i>disable</i>	Disable HTTP request passing to ICAP server.														
<i>enable</i>	Enable HTTP request passing to ICAP server.															
request-failure	Action to take if the ICAP server cannot be contacted when processing an HTTP request.	option	-	error												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>error</i></td><td>Error.</td></tr><tr><td><i>bypass</i></td><td>Bypass.</td></tr></table>	Option	Description	<i>error</i>	Error.	<i>bypass</i>	Bypass.									
	Option	Description														
	<i>error</i>	Error.														
<i>bypass</i>	Bypass.															



Parameter	Description	Type	Size	Default						
request-path	Path component of the ICAP URI that identifies the HTTP request processing service.	string	Maximum length: 127							
request-server	ICAP server to use for an HTTP request.	string	Maximum length: 35							
respmod-default-action	Default action to ICAP response modification (respmod) processing.	option	-	forward						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>forward</i></td><td>Forward response to icap server unless a rule specifies not to.</td></tr><tr><td><i>bypass</i></td><td>Don't forward request to icap server unless a rule specifies to forward the request.</td></tr></table>				Option	Description	<i>forward</i>	Forward response to icap server unless a rule specifies not to.	<i>bypass</i>	Don't forward request to icap server unless a rule specifies to forward the request.
Option	Description									
<i>forward</i>	Forward response to icap server unless a rule specifies not to.									
<i>bypass</i>	Don't forward request to icap server unless a rule specifies to forward the request.									
response	Enable/disable whether an HTTP response is passed to an ICAP server.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable HTTP response passing to ICAP server.</td></tr><tr><td><i>enable</i></td><td>Enable HTTP response passing to ICAP server.</td></tr></table>				Option	Description	<i>disable</i>	Disable HTTP response passing to ICAP server.	<i>enable</i>	Enable HTTP response passing to ICAP server.
Option	Description									
<i>disable</i>	Disable HTTP response passing to ICAP server.									
<i>enable</i>	Enable HTTP response passing to ICAP server.									
response-failure	Action to take if the ICAP server cannot be contacted when processing an HTTP response.	option	-	error						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>error</i></td><td>Error.</td></tr><tr><td><i>bypass</i></td><td>Bypass.</td></tr></table>				Option	Description	<i>error</i>	Error.	<i>bypass</i>	Bypass.
Option	Description									
<i>error</i>	Error.									
<i>bypass</i>	Bypass.									
response-path	Path component of the ICAP URI that identifies the HTTP response processing service.	string	Maximum length: 127							
response-req-hdr	Enable/disable addition of req-hdr for ICAP response modification (respmod) processing.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Do not add req-hdr for response modification (respmod) processing.</td></tr><tr><td><i>enable</i></td><td>Add req-hdr for response modification (respmod) processing.</td></tr></table>				Option	Description	<i>disable</i>	Do not add req-hdr for response modification (respmod) processing.	<i>enable</i>	Add req-hdr for response modification (respmod) processing.
Option	Description									
<i>disable</i>	Do not add req-hdr for response modification (respmod) processing.									
<i>enable</i>	Add req-hdr for response modification (respmod) processing.									
response-server	ICAP server to use for an HTTP response.	string	Maximum length: 35							
scan-progress-interval	Scan progress interval value.	integer	Minimum value: 5 Maximum value: 30	10						

Parameter	Description	Type	Size	Default
streaming-content-bypass	Enable/disable bypassing of ICAP server for streaming content.	option	-	disable
Option	Description			
<i>disable</i>	Disable bypassing of ICAP server for streaming content.			
<i>enable</i>	Enable bypassing of ICAP server for streaming content.			

### config icap-headers

Parameter	Description	Type	Size	Default
id	HTTP forwarded header ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
name	HTTP forwarded header name.	string	Maximum length: 79	
content	HTTP header content.	string	Maximum length: 255	
base64-encoding	Enable/disable use of base64 encoding of HTTP content.	option	-	disable
Option	Description			
<i>disable</i>	Disable use of base64 encoding of HTTP content.			
<i>enable</i>	Enable use of base64 encoding of HTTP content.			

### config respmod-forward-rules

Parameter	Description	Type	Size	Default
name	Address name.	string	Maximum length: 63	
host	Address object for the host.	string	Maximum length: 79	
action	Action to be taken for ICAP server.	option	-	forward
Option	Description			
<i>forward</i>	Forward request to ICAP server when this rule is matched.			

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>bypass</i>	Don't forward request to ICAP server when this rule is matched.		
http-resp-status-code <code>	HTTP response status code. HTTP response status code.	integer	Minimum value: 100 Maximum value: 599	1111499412 **

\*\* Values may differ between models.

### config header-group

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
header-name	HTTP header.	string	Maximum length: 79	
header	HTTP header regular expression.	string	Maximum length: 255	
case-sensitivity	Enable/disable case sensitivity when matching header.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Ignore case when matching header.		
	<i>enable</i>	Do not ignore case when matching header.		

## config icap server

Configure ICAP servers.

```
config icap server
  Description: Configure ICAP servers.
  edit <name>
    set ip-address {ipv4-address-any}
    set ip-version [4|6]
    set ip6-address {ipv6-address}
    set max-connections {integer}
    set port {integer}
    set secure [enable|disable]
    set ssl-cert {string}
```

```
next
end
```

## config icap server

Parameter	Description	Type	Size	Default
ip-address	IPv4 address of the ICAP server.	ipv4-address-any	Not Specified	0.0.0.0
ip-version	IP version.	option	-	4
	<div><div>Option</div><div>Description</div></div>			
	4	IPv4 ICAP address.		
	6	IPv6 ICAP address.		
ip6-address	IPv6 address of the ICAP server.	ipv6-address	Not Specified	::
max-connections	Maximum number of concurrent connections to ICAP server. Must not be less than wad-worker-count.	integer	Minimum value: 1 Maximum value: 65535	100
name	Server name.	string	Maximum length: 35	
port	ICAP server port.	integer	Minimum value: 1 Maximum value: 65535	1344
secure	Enable/disable secure connection to ICAP server.	option	-	disable
	<div><div>Option</div><div>Description</div></div>			
	enable	Enable secure connection to ICAP server.		
	disable	Disable secure connection to ICAP server.		
ssl-cert	CA certificate name.	string	Maximum length: 255	

# ips

This section includes syntax for the following commands:

- [config ips custom on page 545](#)
- [config ips decoder on page 547](#)
- [config ips global on page 547](#)
- [config ips rule-settings on page 551](#)
- [config ips rule on page 551](#)
- [config ips sensor on page 554](#)
- [config ips settings on page 558](#)
- [config ips view-map on page 559](#)

## config ips custom

Configure IPS custom signature.

```
config ips custom
  Description: Configure IPS custom signature.
  edit <tag>
    set action [pass|block]
    set application {user}
    set comment {string}
    set location {user}
    set log [disable|enable]
    set log-packet [disable|enable]
    set os {user}
    set protocol {user}
    set rule-id {integer}
    set severity {user}
    set signature {var-string}
    set status [disable|enable]
  next
end
```

## config ips custom

Parameter	Description	Type	Size	Default
action	Default action (pass or block) for this signature.	option	-	pass
	Option	Description		
	<i>pass</i>	Pass or allow matching traffic.		
	<i>block</i>	Block or drop matching traffic.		

Parameter	Description	Type	Size	Default						
application	Applications to be protected. Blank for all applications.	user	Not Specified							
comment	Comment.	string	Maximum length: 63							
location	Protect client or server traffic.	user	Not Specified							
log	Enable/disable logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable logging.</td></tr><tr><td><i>enable</i></td><td>Enable logging.</td></tr></table>				Option	Description	<i>disable</i>	Disable logging.	<i>enable</i>	Enable logging.
	Option	Description								
	<i>disable</i>	Disable logging.								
<i>enable</i>	Enable logging.									
log-packet	Enable/disable packet logging.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable packet logging.</td></tr><tr><td><i>enable</i></td><td>Enable packet logging.</td></tr></table>				Option	Description	<i>disable</i>	Disable packet logging.	<i>enable</i>	Enable packet logging.
	Option	Description								
	<i>disable</i>	Disable packet logging.								
<i>enable</i>	Enable packet logging.									
os	Operating system(s) that the signature protects. Blank for all operating systems.	user	Not Specified							
protocol	Protocol(s) that the signature scans. Blank for all protocols.	user	Not Specified							
rule-id	Signature ID.	integer	Minimum value: 0 Maximum value: 4294967295	0						
severity	Relative severity of the signature, from info to critical. Log messages generated by the signature include the severity.	user	Not Specified							
signature	Custom signature enclosed in single quotes.	var-string	Maximum length: 4095							
status	Enable/disable this signature.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable status.</td></tr><tr><td><i>enable</i></td><td>Enable status.</td></tr></table>				Option	Description	<i>disable</i>	Disable status.	<i>enable</i>	Enable status.
	Option	Description								
	<i>disable</i>	Disable status.								
<i>enable</i>	Enable status.									
tag	Signature tag.	string	Maximum length: 63							

---

## config ips decoder

Configure IPS decoder.

```
config ips decoder
  Description: Configure IPS decoder.
  edit <name>
    config parameter
      Description: IPS group parameters.
      edit <name>
        set value {string}
      next
    end
  next
end
```

### config ips decoder

Parameter	Description	Type	Size	Default
name	Decoder name.	string	Maximum length: 63	

### config parameter

Parameter	Description	Type	Size	Default
name	Parameter name.	string	Maximum length: 31	
value	Parameter value.	string	Maximum length: 199	

## config ips global

Configure IPS global parameter.

```
config ips global
  Description: Configure IPS global parameter.
  set anomaly-mode [periodical|continuous]
  set cp-accel-mode [none|basic|...]
  set database [regular|extended]
  set deep-app-insp-db-limit {integer}
  set deep-app-insp-timeout {integer}
  set engine-count {integer}
  set exclude-signatures [none|industrial]
  set fail-open [enable|disable]
  set ips-reserve-cpu [disable|enable]
  set ngfw-max-scan-range {integer}
  set np-accel-mode [none|basic]
  set packet-log-queue-depth {integer}
  set session-limit-mode [accurate|heuristic]
```

```

set socket-size {integer}
set sync-session-ttl [enable|disable]
config tls-active-probe
    Description: TLS active probe configuration.
    set interface-select-method [auto|sdwan|...]
    set interface {string}
    set vdom {string}
    set source-ip {ipv4-address}
    set source-ip6 {ipv6-address}
end
set traffic-submit [enable|disable]
end

```

## config ips global

Parameter	Description	Type	Size	Default								
anomaly-mode	Global blocking mode for rate-based anomalies.	option	-	continuous								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>periodical</i></td><td>After an anomaly is detected, allow the number of packets per second according to the anomaly configuration.</td></tr><tr><td><i>continuous</i></td><td>Block packets once an anomaly is detected. Overrides individual anomaly settings.</td></tr></table>	Option	Description	<i>periodical</i>	After an anomaly is detected, allow the number of packets per second according to the anomaly configuration.	<i>continuous</i>	Block packets once an anomaly is detected. Overrides individual anomaly settings.					
Option	Description											
<i>periodical</i>	After an anomaly is detected, allow the number of packets per second according to the anomaly configuration.											
<i>continuous</i>	Block packets once an anomaly is detected. Overrides individual anomaly settings.											
cp-accel-mode *	IPS Pattern matching acceleration/offloading to CPx processors.	option	-	advanced								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>CPx acceleration/offloading disabled.</td></tr><tr><td><i>basic</i></td><td>Offload basic pattern matching to CPx processors.</td></tr><tr><td><i>advanced</i></td><td>Offload more types of pattern matching resulting in higher throughput than basic mode. Requires two CP8s or one CP9.</td></tr></table>	Option	Description	<i>none</i>	CPx acceleration/offloading disabled.	<i>basic</i>	Offload basic pattern matching to CPx processors.	<i>advanced</i>	Offload more types of pattern matching resulting in higher throughput than basic mode. Requires two CP8s or one CP9.			
Option	Description											
<i>none</i>	CPx acceleration/offloading disabled.											
<i>basic</i>	Offload basic pattern matching to CPx processors.											
<i>advanced</i>	Offload more types of pattern matching resulting in higher throughput than basic mode. Requires two CP8s or one CP9.											
database	Regular or extended IPS database. Regular protects against the latest common and in-the-wild attacks. Extended includes protection from legacy attacks.	option	-	extended **								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>regular</i></td><td>IPS regular database package.</td></tr><tr><td><i>extended</i></td><td>IPS extended database package.</td></tr></table>	Option	Description	<i>regular</i>	IPS regular database package.	<i>extended</i>	IPS extended database package.					
Option	Description											
<i>regular</i>	IPS regular database package.											
<i>extended</i>	IPS extended database package.											



Parameter	Description	Type	Size	Default						
deep-app-insp-db-limit	Limit on number of entries in deep application inspection database.	integer	Minimum value: 0 Maximum value: 2147483647	0						
deep-app-insp-timeout	Timeout for Deep application inspection.	integer	Minimum value: 0 Maximum value: 2147483647	0						
engine-count	Number of IPS engines running. If set to the default value of 0, FortiOS sets the number to optimize performance depending on the number of CPU cores.	integer	Minimum value: 0 Maximum value: 255	0						
exclude-signatures	Excluded signatures.	option	-	industrial						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>No signatures excluded.</td></tr><tr><td><i>industrial</i></td><td>Exclude industrial signatures.</td></tr></table>				Option	Description	<i>none</i>	No signatures excluded.	<i>industrial</i>	Exclude industrial signatures.
Option	Description									
<i>none</i>	No signatures excluded.									
<i>industrial</i>	Exclude industrial signatures.									
fail-open	Enable to allow traffic if the IPS buffer is full. Default is disable and IPS traffic is blocked when the IPS buffer is full.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable IPS fail open.</td></tr><tr><td><i>disable</i></td><td>Disable IPS fail open.</td></tr></table>				Option	Description	<i>enable</i>	Enable IPS fail open.	<i>disable</i>	Disable IPS fail open.
Option	Description									
<i>enable</i>	Enable IPS fail open.									
<i>disable</i>	Disable IPS fail open.									
ips-reserve-cpu *	Enable/disable IPS daemon's use of CPUs other than CPU 0	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable IPS daemon's use of CPUs other than CPU 0 (all daemons run on all CPUs).</td></tr><tr><td><i>enable</i></td><td>Enable IPS daemon's use of CPUs other than CPU 0.</td></tr></table>				Option	Description	<i>disable</i>	Disable IPS daemon's use of CPUs other than CPU 0 (all daemons run on all CPUs).	<i>enable</i>	Enable IPS daemon's use of CPUs other than CPU 0.
Option	Description									
<i>disable</i>	Disable IPS daemon's use of CPUs other than CPU 0 (all daemons run on all CPUs).									
<i>enable</i>	Enable IPS daemon's use of CPUs other than CPU 0.									
ngfw-max-scan-range	NGFW policy-mode app detection threshold.	integer	Minimum value: 0 Maximum value: 4294967295	4096						

Parameter	Description	Type	Size	Default						
np-accel-mode *	Acceleration mode for IPS processing by NPx processors.	option	-	basic						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>NPx acceleration disabled.</td></tr><tr><td><i>basic</i></td><td>NPx acceleration enabled.</td></tr></table>	Option	Description	<i>none</i>	NPx acceleration disabled.	<i>basic</i>	NPx acceleration enabled.			
Option	Description									
<i>none</i>	NPx acceleration disabled.									
<i>basic</i>	NPx acceleration enabled.									
packet-log-queue-depth	Packet/pcap log queue depth per IPS engine.	integer	Minimum value: 128 Maximum value: 4096	128						
session-limit-mode	Method of counting concurrent sessions used by session limit anomalies. Choose between greater accuracy (accurate) or improved performance (heuristics).	option	-	heuristic						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>accurate</i></td><td>Accurately count concurrent sessions, demands more resources.</td></tr><tr><td><i>heuristic</i></td><td>Use heuristics to estimate the number of concurrent sessions. Acceptable in most cases.</td></tr></table>	Option	Description	<i>accurate</i>	Accurately count concurrent sessions, demands more resources.	<i>heuristic</i>	Use heuristics to estimate the number of concurrent sessions. Acceptable in most cases.			
Option	Description									
<i>accurate</i>	Accurately count concurrent sessions, demands more resources.									
<i>heuristic</i>	Use heuristics to estimate the number of concurrent sessions. Acceptable in most cases.									
socket-size	IPS socket buffer size. Max and default value depend on available memory. Can be changed to tune performance.	integer	Minimum value: 0 Maximum value: 256 **	128 **						
sync-session-ttl	Enable/disable use of kernel session TTL for IPS sessions.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable use of kernel session TTL for IPS sessions.</td></tr><tr><td><i>disable</i></td><td>Disable use of kernel session TTL for IPS sessions.</td></tr></table>	Option	Description	<i>enable</i>	Enable use of kernel session TTL for IPS sessions.	<i>disable</i>	Disable use of kernel session TTL for IPS sessions.			
Option	Description									
<i>enable</i>	Enable use of kernel session TTL for IPS sessions.									
<i>disable</i>	Disable use of kernel session TTL for IPS sessions.									
traffic-submit	Enable/disable submitting attack data found by this FortiGate to FortiGuard.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable traffic submit.</td></tr><tr><td><i>disable</i></td><td>Disable traffic submit.</td></tr></table>	Option	Description	<i>enable</i>	Enable traffic submit.	<i>disable</i>	Disable traffic submit.			
Option	Description									
<i>enable</i>	Enable traffic submit.									
<i>disable</i>	Disable traffic submit.									

\* This parameter may not exist in some models.

\*\* Values may differ between models.

## config tls-active-probe

Parameter	Description	Type	Size	Default
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto
	<b>Option</b>	<b>Description</b>		
	<i>auto</i>	Set outgoing interface automatically.		
	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.		
	<i>specify</i>	Set outgoing interface manually.		
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	
vdom	Virtual domain name for TLS active probe.	string	Maximum length: 31	
source-ip	Source IP address used for TLS active probe.	ipv4-address	Not Specified	0.0.0.0
source-ip6	Source IPv6 address used for TLS active probe.	ipv6-address	Not Specified	::

## config ips rule-settings

Configure IPS rule setting.

```
config ips rule-settings
    Description: Configure IPS rule setting.
    edit <id>
        next
    end
```

## config ips rule-settings

Parameter	Description	Type	Size	Default
id	Rule ID.	integer	Minimum value: 0 Maximum value: 4294967295	0

## config ips rule

Configure IPS rules.

```

config ips rule
  Description: Configure IPS rules.
  edit <name>
    set action [pass|block]
    set application {user}
    set date {integer}
    set group {string}
    set location {user}
    set log [disable|enable]
    set log-packet [disable|enable]
    config metadata
      Description: Meta data.
      edit <id>
        set metaid {integer}
        set valueid {integer}
      next
    end
    set os {user}
    set rev {integer}
    set rule-id {integer}
    set service {user}
    set severity {user}
    set status [disable|enable]
  next
end

```

## config ips rule

Parameter	Description	Type	Size	Default
action	Action.	option	-	pass
	Option	Description		
	pass	Pass or allow matching traffic.		
	block	Block or drop matching traffic.		
application	Vulnerable applications.	user	Not Specified	
date	Date.	integer	Minimum value: 0 Maximum value: 4294967295	0
group	Group.	string	Maximum length: 63	
location	Vulnerable location.	user	Not Specified	
log	Enable/disable logging.	option	-	enable

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable logging.		
	<i>enable</i>	Enable logging.		
log-packet	Enable/disable packet logging.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable packet logging.		
	<i>enable</i>	Enable packet logging.		
name	Rule name.	string	Maximum length: 63	
os	Vulnerable operation systems.	user	Not Specified	
rev	Revision.	integer	Minimum value: 0 Maximum value: 4294967295	0
rule-id	Rule ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
service	Vulnerable service.	user	Not Specified	
severity	Severity.	user	Not Specified	
status	Enable/disable status.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		

### config metadata

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0

Parameter	Description	Type	Size	Default
metaid	Meta ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
valueid	Value ID.	integer	Minimum value: 0 Maximum value: 4294967295	0

## config ips sensor

Configure IPS sensor.

```

config ips sensor
  Description: Configure IPS sensor.
  edit <name>
    set block-malicious-url [disable|enable]
    set comment {var-string}
    config entries
      Description: IPS sensor filter.
      edit <id>
        set rule <id1>, <id2>, ...
        set location {user}
        set severity {user}
        set protocol {user}
        set os {user}
        set application {user}
        set cve <cve-entry1>, <cve-entry2>, ...
        set status [disable|enable|...]
        set log [disable|enable]
        set log-packet [disable|enable]
        set log-attack-context [disable|enable]
        set action [pass|block|...]
        set rate-count {integer}
        set rate-duration {integer}
        set rate-mode [periodical|continuous]
        set rate-track [none|src-ip|...]
        config exempt-ip
          Description: Traffic from selected source or destination IP addresses is
exempt from this signature.
          edit <id>
            set src-ip {ipv4-classnet}
            set dst-ip {ipv4-classnet}
          next
        end
        set quarantine [none|attacker]
        set quarantine-expiry {user}
        set quarantine-log [disable|enable]
      next
    end
  next

```

```

        end
        set extended-log [enable|disable]
        set replacemsg-group {string}
        set scan-botnet-connections [disable|block|...]
    next
end

```

## config ips sensor

Parameter	Description	Type	Size	Default
block-malicious-url	Enable/disable malicious URL blocking.	option	-	disable
	<b>Option</b>		<b>Description</b>	
	<i>disable</i>		Disable malicious URL blocking.	
	<i>enable</i>		Enable malicious URL blocking.	
comment	Comment.	var-string	Maximum length: 255	
extended-log	Enable/disable extended logging.	option	-	disable
	<b>Option</b>		<b>Description</b>	
	<i>enable</i>		Enable setting.	
	<i>disable</i>		Disable setting.	
name	Sensor name.	string	Maximum length: 35	
replacemsg-group	Replacement message group.	string	Maximum length: 35	
scan-botnet-connections	Block or monitor connections to Botnet servers, or disable Botnet scanning.	option	-	disable
	<b>Option</b>		<b>Description</b>	
	<i>disable</i>		Do not scan connections to botnet servers.	
	<i>block</i>		Block connections to botnet servers.	
	<i>monitor</i>		Log connections to botnet servers.	

## config entries

Parameter	Description	Type	Size	Default								
id	Rule ID in IPS database.	integer	Minimum value: 0 Maximum value: 4294967295	0								
rule <id>	Identifies the predefined or custom IPS signatures to add to the sensor. Rule IPS.	integer	Minimum value: 0 Maximum value: 4294967295									
location	Protect client or server traffic.	user	Not Specified	all								
severity	Relative severity of the signature, from info to critical. Log messages generated by the signature include the severity.	user	Not Specified	all								
protocol	Protocols to be examined. Use all for every protocol and other for unlisted protocols.	user	Not Specified	all								
os	Operating systems to be protected. Use all for every operating system and other for unlisted operating systems.	user	Not Specified	all								
application	Operating systems to be protected. Use all for every application and other for unlisted application.	user	Not Specified	all								
cve <cve-entry>	List of CVE IDs of the signatures to add to the sensor. CVE IDs or CVE wildcards.	string	Maximum length: 19									
status	Status of the signatures included in filter. Only those filters with a status to enable are used.	option	-	default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable status of selected rules.</td></tr><tr><td>enable</td><td>Enable status of selected rules.</td></tr><tr><td>default</td><td>Default.</td></tr></table>				Option	Description	disable	Disable status of selected rules.	enable	Enable status of selected rules.	default	Default.
Option	Description											
disable	Disable status of selected rules.											
enable	Enable status of selected rules.											
default	Default.											
log	Enable/disable logging of signatures included in filter.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable logging of selected rules.</td></tr><tr><td>enable</td><td>Enable logging of selected rules.</td></tr></table>				Option	Description	disable	Disable logging of selected rules.	enable	Enable logging of selected rules.		
Option	Description											
disable	Disable logging of selected rules.											
enable	Enable logging of selected rules.											



Parameter	Description	Type	Size	Default										
log-packet	Enable/disable packet logging. Enable to save the packet that triggers the filter. You can download the packets in pcap format for diagnostic use.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable packet logging of selected rules.</td></tr><tr><td><i>enable</i></td><td>Enable packet logging of selected rules.</td></tr></table>	Option	Description	<i>disable</i>	Disable packet logging of selected rules.	<i>enable</i>	Enable packet logging of selected rules.							
Option	Description													
<i>disable</i>	Disable packet logging of selected rules.													
<i>enable</i>	Enable packet logging of selected rules.													
log-attack-context	Enable/disable logging of attack context: URL buffer, header buffer, body buffer, packet buffer.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable logging of detailed attack context.</td></tr><tr><td><i>enable</i></td><td>Enable logging of detailed attack context.</td></tr></table>	Option	Description	<i>disable</i>	Disable logging of detailed attack context.	<i>enable</i>	Enable logging of detailed attack context.							
Option	Description													
<i>disable</i>	Disable logging of detailed attack context.													
<i>enable</i>	Enable logging of detailed attack context.													
action	Action taken with traffic in which signatures are detected.	option	-	default										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>pass</i></td><td>Pass or allow matching traffic.</td></tr><tr><td><i>block</i></td><td>Block or drop matching traffic.</td></tr><tr><td><i>reset</i></td><td>Reset sessions for matching traffic.</td></tr><tr><td><i>default</i></td><td>Pass or drop matching traffic, depending on the default action of the signature.</td></tr></table>	Option	Description	<i>pass</i>	Pass or allow matching traffic.	<i>block</i>	Block or drop matching traffic.	<i>reset</i>	Reset sessions for matching traffic.	<i>default</i>	Pass or drop matching traffic, depending on the default action of the signature.			
Option	Description													
<i>pass</i>	Pass or allow matching traffic.													
<i>block</i>	Block or drop matching traffic.													
<i>reset</i>	Reset sessions for matching traffic.													
<i>default</i>	Pass or drop matching traffic, depending on the default action of the signature.													
rate-count	Count of the rate.	integer	Minimum value: 0 Maximum value: 65535	0										
rate-duration	Duration (sec) of the rate.	integer	Minimum value: 1 Maximum value: 65535	60										
rate-mode	Rate limit mode.	option	-	continuous										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>periodical</i></td><td>Allow configured number of packets every rate-duration.</td></tr><tr><td><i>continuous</i></td><td>Block packets once the rate is reached.</td></tr></table>	Option	Description	<i>periodical</i>	Allow configured number of packets every rate-duration.	<i>continuous</i>	Block packets once the rate is reached.							
Option	Description													
<i>periodical</i>	Allow configured number of packets every rate-duration.													
<i>continuous</i>	Block packets once the rate is reached.													
rate-track	Track the packet protocol field.	option	-	none										

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	none		
	<i>src-ip</i>	Source IP.		
	<i>dest-ip</i>	Destination IP.		
	<i>dhcp-client-mac</i>	DHCP client.		
	<i>dns-domain</i>	DNS domain.		
quarantine	Quarantine method.	option	-	none
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	Quarantine is disabled.		
	<i>attacker</i>	Block all traffic sent from attacker's IP address. The attacker's IP address is also added to the banned user list. The target's address is not affected.		
quarantine-expiry	Duration of quarantine.. Requires quarantine set to attacker.	user	Not Specified	5m
quarantine-log	Enable/disable quarantine logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable quarantine logging.		
	<i>enable</i>	Enable quarantine logging.		

### config exempt-ip

Parameter	Description	Type	Size	Default
id	Exempt IP ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
src-ip	Source IP address and netmask (applies to packet matching the signature).	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0
dst-ip	Destination IP address and netmask (applies to packet matching the signature).	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0

## config ips settings

Configure IPS VDOM parameter.

```

config ips settings
    Description: Configure IPS VDOM parameter.
    set ips-packet-quota {integer}
    set packet-log-history {integer}
    set packet-log-memory {integer}
    set packet-log-post-attack {integer}
end

```

## config ips settings

Parameter	Description	Type	Size	Default
ips-packet-quota	Maximum amount of disk space in MB for logged packets when logging to disk. Range depends on disk size.	integer	Minimum value: 0 Maximum value: 4294967295	0
packet-log-history	Number of packets to capture before and including the one in which the IPS signature is detected.	integer	Minimum value: 1 Maximum value: 255	1
packet-log-memory	Maximum memory can be used by packet log.	integer	Minimum value: 64 Maximum value: 8192	256
packet-log-post-attack	Number of packets to log after the IPS signature is detected.	integer	Minimum value: 0 Maximum value: 255	0

## config ips view-map

Configure IPS view-map.

```

config ips view-map
    Description: Configure IPS view-map.
    edit <id>
        set id-policy-id {integer}
        set policy-id {integer}
        set vdom-id {integer}
        set which [firewall|interface|...]
    next
end

```

## config ips view-map

Parameter	Description	Type	Size	Default
id	View ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
id-policy-id	ID-based policy ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
policy-id	Policy ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
vdom-id	VDOM ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
which	Policy.	option	-	firewall
		Option	Description	
		<i>firewall</i>	Firewall policy.	
		<i>interface</i>	Interface policy.	
		<i>interface6</i>	Interface policy6.	
		<i>sniffer</i>	Sniffer policy.	
		<i>sniffer6</i>	Sniffer policy6.	
		<i>explicit</i>	explicit proxy policy.	

# log

This section includes syntax for the following commands:

- [config log custom-field on page 562](#)
- [config log disk filter on page 563](#)
- [config log disk setting on page 566](#)
- [config log eventfilter on page 571](#)
- [config log fortianalyzer-cloud filter on page 574](#)
- [config log fortianalyzer-cloud override-filter on page 578](#)
- [config log fortianalyzer-cloud override-setting on page 581](#)
- [config log fortianalyzer-cloud setting on page 581](#)
- [config log fortianalyzer2 filter on page 585](#)
- [config log fortianalyzer2 override-filter on page 588](#)
- [config log fortianalyzer2 override-setting on page 592](#)
- [config log fortianalyzer2 setting on page 596](#)
- [config log fortianalyzer3 filter on page 600](#)
- [config log fortianalyzer3 override-filter on page 603](#)
- [config log fortianalyzer3 override-setting on page 607](#)
- [config log fortianalyzer3 setting on page 611](#)
- [config log fortianalyzer filter on page 615](#)
- [config log fortianalyzer override-filter on page 618](#)
- [config log fortianalyzer override-setting on page 621](#)
- [config log fortianalyzer setting on page 625](#)
- [config log fortiguard filter on page 629](#)
- [config log fortiguard override-filter on page 632](#)
- [config log fortiguard override-setting on page 636](#)
- [config log fortiguard setting on page 637](#)
- [config log gui-display on page 640](#)
- [config log memory filter on page 641](#)
- [config log memory global-setting on page 644](#)
- [config log memory setting on page 645](#)
- [config log npu-server on page 645](#)
- [config log null-device filter on page 649](#)
- [config log null-device setting on page 652](#)
- [config log setting on page 653](#)
- [config log syslogd2 filter on page 657](#)
- [config log syslogd2 override-filter on page 660](#)
- [config log syslogd2 override-setting on page 664](#)
- [config log syslogd2 setting on page 667](#)
- [config log syslogd3 filter on page 671](#)

- [config log syslogd3 override-filter on page 674](#)
- [config log syslogd3 override-setting on page 678](#)
- [config log syslogd3 setting on page 681](#)
- [config log syslogd4 filter on page 685](#)
- [config log syslogd4 override-filter on page 688](#)
- [config log syslogd4 override-setting on page 692](#)
- [config log syslogd4 setting on page 695](#)
- [config log syslogd filter on page 699](#)
- [config log syslogd override-filter on page 702](#)
- [config log syslogd override-setting on page 706](#)
- [config log syslogd setting on page 709](#)
- [config log tacacs+accounting2 filter on page 713](#)
- [config log tacacs+accounting2 setting on page 714](#)
- [config log tacacs+accounting3 filter on page 714](#)
- [config log tacacs+accounting3 setting on page 715](#)
- [config log tacacs+accounting filter on page 716](#)
- [config log tacacs+accounting setting on page 717](#)
- [config log threat-weight on page 717](#)
- [config log webtrends filter on page 728](#)
- [config log webtrends setting on page 731](#)

## config log custom-field

Configure custom log fields.

```
config log custom-field
    Description: Configure custom log fields.
    edit <id>
        set name {string}
        set value {string}
    next
end
```

### config log custom-field

Parameter	Description	Type	Size	Default
id	Field ID string.	string	Maximum length: 35	
name	Field name (max: 15 characters).	string	Maximum length: 15	
value	Field value (max: 15 characters).	string	Maximum length: 15	

## config log disk filter

Configure filters for local disk logging. Use these filters to determine the log messages to record according to severity and type.

```
config log disk filter
    Description: Configure filters for local disk logging. Use these filters to determine
the log messages to record according to severity and type.
    set anomaly [enable|disable]
    set dlp-archive [enable|disable]
    set forward-traffic [enable|disable]
    config free-style
        Description: Free style filters.
        edit <id>
            set category [traffic|event|...]
            set filter {string}
            set filter-type [include|exclude]
        next
    end
    set gtp [enable|disable]
    set local-traffic [enable|disable]
    set multicast-traffic [enable|disable]
    set severity [emergency|alert|...]
    set sniffer-traffic [enable|disable]
    set voip [enable|disable]
    set ztna-traffic [enable|disable]
end
```

## config log disk filter

Parameter	Description	Type	Size	Default
anomaly	Enable/disable anomaly logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable anomaly logging.		
	<i>disable</i>	Disable anomaly logging.		
dlp-archive *	Enable/disable DLP archive logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable DLP archive logging.		
	<i>disable</i>	Disable DLP archive logging.		
forward-traffic	Enable/disable forward traffic logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable forward traffic logging.		
	<i>disable</i>	Disable forward traffic logging.		

Parameter	Description	Type	Size	Default																		
gtp *	Enable/disable GTP messages logging.	option	-	enable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable GTP messages logging.</td></tr><tr><td><i>disable</i></td><td>Disable GTP messages logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable GTP messages logging.	<i>disable</i>	Disable GTP messages logging.															
Option	Description																					
<i>enable</i>	Enable GTP messages logging.																					
<i>disable</i>	Disable GTP messages logging.																					
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable local in or out traffic logging.</td></tr><tr><td><i>disable</i></td><td>Disable local in or out traffic logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable local in or out traffic logging.	<i>disable</i>	Disable local in or out traffic logging.															
Option	Description																					
<i>enable</i>	Enable local in or out traffic logging.																					
<i>disable</i>	Disable local in or out traffic logging.																					
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable multicast traffic logging.</td></tr><tr><td><i>disable</i></td><td>Disable multicast traffic logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable multicast traffic logging.	<i>disable</i>	Disable multicast traffic logging.															
Option	Description																					
<i>enable</i>	Enable multicast traffic logging.																					
<i>disable</i>	Disable multicast traffic logging.																					
severity	Log to disk every message above and including this severity level.	option	-	information																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>emergency</i></td><td>Emergency level.</td></tr><tr><td><i>alert</i></td><td>Alert level.</td></tr><tr><td><i>critical</i></td><td>Critical level.</td></tr><tr><td><i>error</i></td><td>Error level.</td></tr><tr><td><i>warning</i></td><td>Warning level.</td></tr><tr><td><i>notification</i></td><td>Notification level.</td></tr><tr><td><i>information</i></td><td>Information level.</td></tr><tr><td><i>debug</i></td><td>Debug level.</td></tr></table>	Option	Description	<i>emergency</i>	Emergency level.	<i>alert</i>	Alert level.	<i>critical</i>	Critical level.	<i>error</i>	Error level.	<i>warning</i>	Warning level.	<i>notification</i>	Notification level.	<i>information</i>	Information level.	<i>debug</i>	Debug level.			
Option	Description																					
<i>emergency</i>	Emergency level.																					
<i>alert</i>	Alert level.																					
<i>critical</i>	Critical level.																					
<i>error</i>	Error level.																					
<i>warning</i>	Warning level.																					
<i>notification</i>	Notification level.																					
<i>information</i>	Information level.																					
<i>debug</i>	Debug level.																					
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable sniffer traffic logging.</td></tr><tr><td><i>disable</i></td><td>Disable sniffer traffic logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable sniffer traffic logging.	<i>disable</i>	Disable sniffer traffic logging.															
Option	Description																					
<i>enable</i>	Enable sniffer traffic logging.																					
<i>disable</i>	Disable sniffer traffic logging.																					
voip	Enable/disable VoIP logging.	option	-	enable																		



Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable VoIP logging.		
	<i>disable</i>	Disable VoIP logging.		
ztna-traffic	Enable/disable ztna traffic logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable ztna traffic logging.		
	<i>disable</i>	Disable ztna traffic logging.		

\* This parameter may not exist in some models.

### config free-style

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
category	Log category.	option	-	traffic
	<b>Option</b>	<b>Description</b>		
	<i>traffic</i>	Traffic log.		
	<i>event</i>	Event log.		
	<i>virus</i>	Antivirus log.		
	<i>webfilter</i>	Web filter log.		
	<i>attack</i>	Attack log.		
	<i>spam</i>	Antispam log.		
	<i>anomaly</i>	Anomaly log.		
	<i>voip</i>	VoIP log.		
	<i>dlp</i>	DLP log.		
	<i>app-ctrl</i>	Application control log.		
	<i>waf</i>	Web application firewall log.		
	<i>dns</i>	DNS detail log.		

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>ssh</i>	SSH log.		
	<i>ssl</i>	SSL log.		
	<i>file-filter</i>	File filter log.		
	<i>icap</i>	ICAP log.		
filter	Free style filter string.	string	Maximum length: 1023	
filter-type	Include/exclude logs that match the filter.	option	-	include
	<b>Option</b>	<b>Description</b>		
	<i>include</i>	Include logs that match the filter.		
	<i>exclude</i>	Exclude logs that match the filter.		

## config log disk setting

Settings for local disk logging.

```

config log disk setting
    Description: Settings for local disk logging.
    set diskfull [overwrite|nolog]
    set dlp-archive-quota {integer}
    set full-final-warning-threshold {integer}
    set full-first-warning-threshold {integer}
    set full-second-warning-threshold {integer}
    set interface {string}
    set interface-select-method [auto|sdwan|...]
    set ips-archive [enable|disable]
    set log-quota {integer}
    set max-log-file-size {integer}
    set max-policy-packet-capture-size {integer}
    set maximum-log-age {integer}
    set report-quota {integer}
    set roll-day {option1}, {option2}, ...
    set roll-schedule [daily|weekly]
    set roll-time {user}
    set source-ip {ipv4-address}
    set status [enable|disable]
    set upload [enable|disable]
    set upload-delete-files [enable|disable]
    set upload-destination {option}
    set upload-ssl-conn [default|high|...]
    set uploadaddir {string}
    set uploadip {ipv4-address}
    set uploadpass {password}
    set uploadport {integer}

```

```

set uploadsched [disable|enable]
set uploadtime {user}
set uploadtype {option1}, {option2}, ...
set uploaduser {string}
end

```

## config log disk setting

Parameter	Description	Type	Size	Default
diskfull	Action to take when disk is full. The system can overwrite the oldest log messages or stop logging when the disk is full.	option	-	overwrite
	<b>Option</b>	<b>Description</b>		
	<i>overwrite</i>	Overwrite the oldest logs when the log disk is full.		
	<i>nolog</i>	Stop logging when the log disk is full.		
dlp-archive-quota	DLP archive quota (MB).	integer	Minimum value: 0 Maximum value: 4294967295	0
full-final-warning-threshold	Log full final warning threshold as a percent.	integer	Minimum value: 3 Maximum value: 100	95
full-first-warning-threshold	Log full first warning threshold as a percent.	integer	Minimum value: 1 Maximum value: 98	75
full-second-warning-threshold	Log full second warning threshold as a percent.	integer	Minimum value: 2 Maximum value: 99	90
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto
	<b>Option</b>	<b>Description</b>		
	<i>auto</i>	Set outgoing interface automatically.		
	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.		
	<i>specify</i>	Set outgoing interface manually.		

Parameter	Description	Type	Size	Default
ips-archive	Enable/disable IPS packet archiving to the local disk.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable IPS packet archiving.		
	<i>disable</i>	Disable IPS packet archiving.		
log-quota	Disk log quota (MB).	integer	Minimum value: 0 Maximum value: 4294967295	0
max-log-file-size	Maximum log file size before rolling.	integer	Minimum value: 1 Maximum value: 100	20
max-policy-packet-capture-size	Maximum size of policy sniffer in MB (0 means unlimited).	integer	Minimum value: 0 Maximum value: 4294967295	100
maximum-log-age	Delete log files older than (days).	integer	Minimum value: 0 Maximum value: 3650	7
report-quota *	Report db quota (MB).	integer	Minimum value: 0 Maximum value: 4294967295	0
roll-day	Day of week on which to roll log file.	option	-	sunday
	<b>Option</b>	<b>Description</b>		
	<i>sunday</i>	Sunday		
	<i>monday</i>	Monday		
	<i>tuesday</i>	Tuesday		
	<i>wednesday</i>	Wednesday		
	<i>thursday</i>	Thursday		
	<i>friday</i>	Friday		

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>saturday</i>	Saturday		
roll-schedule	Frequency to check log file for rolling.	option	-	daily
	<b>Option</b>	<b>Description</b>		
	<i>daily</i>	Check the log file once a day.		
	<i>weekly</i>	Check the log file once a week.		
roll-time	Time of day to roll the log file (hh:mm).	user	Not Specified	
source-ip	Source IP address to use for uploading disk log files.	ipv4-address	Not Specified	0.0.0.0
status	Enable/disable local disk logging.	option	-	disable **
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Log to local disk.		
	<i>disable</i>	Do not log to local disk.		
upload	Enable/disable uploading log files when they are rolled.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable uploading log files when they are rolled.		
	<i>disable</i>	Disable uploading log files when they are rolled.		
upload-delete-files	Delete log files after uploading.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Delete log files after uploading.		
	<i>disable</i>	Do not delete log files after uploading.		
upload-destination	The type of server to upload log files to. Only FTP is currently supported.	option	-	ftp-server
	<b>Option</b>	<b>Description</b>		
	<i>ftp-server</i>	Upload rolled log files to an FTP server.		
upload-ssl-conn	Enable/disable encrypted FTPS communication to upload log files.	option	-	default

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>default</i>	FTPS with high and medium encryption algorithms.		
	<i>high</i>	FTPS with high encryption algorithms.		
	<i>low</i>	FTPS with low encryption algorithms.		
	<i>disable</i>	Disable FTPS communication.		
uploadaddr	The remote directory on the FTP server to upload log files to.	string	Maximum length: 63	
uploadip	IP address of the FTP server to upload log files to.	ipv4-address	Not Specified	0.0.0.0
uploadpass	Password required to log into the FTP server to upload disk log files.	password	Not Specified	
uploadport	TCP port to use for communicating with the FTP server.	integer	Minimum value: 0 Maximum value: 65535	21
uploadsched	Set the schedule for uploading log files to the FTP server.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Upload when rolling.		
	<i>enable</i>	Scheduled upload.		
uploadtime	Time of day at which log files are uploaded if uploadsched is enabled (hh:mm or hh).	user	Not Specified	
uploadtype	Types of log files to upload. Separate multiple entries with a space.	option	-	traffic event virus webfilter IPS emailfilter dlp-archive anomaly voip dlp app-ctrl waf dns ssh ssl **
	<b>Option</b>	<b>Description</b>		
	<i>traffic</i>	Upload traffic log.		

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>event</i>	Upload event log.		
	<i>virus</i>	Upload anti-virus log.		
	<i>webfilter</i>	Upload web filter log.		
	<i>IPS</i>	Upload IPS log.		
	<i>emailfilter</i>	Upload spam filter log.		
	<i>dlp-archive</i>	Upload DLP archive.		
	<i>anomaly</i>	Upload anomaly log.		
	<i>voip</i>	Upload VoIP log.		
	<i>dlp</i>	Upload DLP log.		
	<i>app-ctrl</i>	Upload application control log.		
	<i>waf</i>	Upload web application firewall log.		
	<i>dns</i>	Upload DNS log.		
	<i>ssh</i>	Upload SSH log.		
	<i>ssl</i>	Upload SSL log.		
	<i>file-filter</i>	Upload file-filter log.		
	<i>icap</i>	Upload ICAP log.		
uploaduser	Username required to log into the FTP server to upload disk log files.	string	Maximum length: 35	

\* This parameter may not exist in some models.

\*\* Values may differ between models.

## config log eventfilter

Configure log event filters.

```
config log eventfilter
    Description: Configure log event filters.
    set cifs [enable|disable]
    set connector [enable|disable]
    set endpoint [enable|disable]
    set event [enable|disable]
    set fortiextender [enable|disable]
    set ha [enable|disable]
    set rest-api [enable|disable]
    set router [enable|disable]
    set sdwan [enable|disable]
    set security-rating [enable|disable]
```

```

set switch-controller [enable|disable]
set system [enable|disable]
set user [enable|disable]
set vpn [enable|disable]
set wan-opt [enable|disable]
set wireless-activity [enable|disable]
end

```

## config log eventfilter

Parameter	Description	Type	Size	Default						
cifs	Enable/disable CIFS logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable CIFS logging.</td></tr><tr><td><i>disable</i></td><td>Disable CIFS logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable CIFS logging.	<i>disable</i>	Disable CIFS logging.			
Option	Description									
<i>enable</i>	Enable CIFS logging.									
<i>disable</i>	Disable CIFS logging.									
connector	Enable/disable SDN connector logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable SDN connector logging.</td></tr><tr><td><i>disable</i></td><td>Disable SDN connector logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable SDN connector logging.	<i>disable</i>	Disable SDN connector logging.			
Option	Description									
<i>enable</i>	Enable SDN connector logging.									
<i>disable</i>	Disable SDN connector logging.									
endpoint	Enable/disable endpoint event logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable endpoint event logging.</td></tr><tr><td><i>disable</i></td><td>Disable endpoint event logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable endpoint event logging.	<i>disable</i>	Disable endpoint event logging.			
Option	Description									
<i>enable</i>	Enable endpoint event logging.									
<i>disable</i>	Disable endpoint event logging.									
event	Enable/disable event logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable event logging.</td></tr><tr><td><i>disable</i></td><td>Disable event logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable event logging.	<i>disable</i>	Disable event logging.			
Option	Description									
<i>enable</i>	Enable event logging.									
<i>disable</i>	Disable event logging.									
fortiextender	Enable/disable FortiExtender logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Forti-Extender logging.</td></tr><tr><td><i>disable</i></td><td>Disable Forti-Extender logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable Forti-Extender logging.	<i>disable</i>	Disable Forti-Extender logging.			
Option	Description									
<i>enable</i>	Enable Forti-Extender logging.									
<i>disable</i>	Disable Forti-Extender logging.									
ha	Enable/disable ha event logging.	option	-	enable						



Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable ha event logging.		
	<i>disable</i>	Disable ha event logging.		
rest-api	Enable/disable REST API logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable REST API logging.		
	<i>disable</i>	Disable REST API logging.		
router	Enable/disable router event logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable router event logging.		
	<i>disable</i>	Disable router event logging.		
sdwan	Enable/disable SD-WAN logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable SD-WAN logging.		
	<i>disable</i>	Disable SD-WAN logging.		
security-rating	Enable/disable Security Rating result logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable Security Fabric audit result logging.		
	<i>disable</i>	Disable Security Fabric audit result logging.		
switch-controller	Enable/disable Switch-Controller logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable Switch-Controller logging.		
	<i>disable</i>	Disable Switch-Controller logging.		
system	Enable/disable system event logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable system event logging.		
	<i>disable</i>	Disable system event logging.		

Parameter	Description	Type	Size	Default
user	Enable/disable user authentication event logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable user authentication event logging.		
	<i>disable</i>	Disable user authentication event logging.		
vpn	Enable/disable VPN event logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable VPN event logging.		
	<i>disable</i>	Disable VPN event logging.		
wan-opt	Enable/disable WAN optimization event logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable WAN optimization event logging.		
	<i>disable</i>	Disable WAN optimization event logging.		
wireless-activity	Enable/disable wireless event logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable wireless event logging.		
	<i>disable</i>	Disable wireless event logging.		

## config log fortianalyzer-cloud filter

Filters for FortiAnalyzer Cloud.

```
config log fortianalyzer-cloud filter
  Description: Filters for FortiAnalyzer Cloud.
  set anomaly [enable|disable]
  set dlp-archive [enable|disable]
  set forward-traffic [enable|disable]
  config free-style
    Description: Free style filters.
    edit <id>
      set category [traffic|event|...]
      set filter {string}
      set filter-type [include|exclude]
    next
  end
  set gtp [enable|disable]
  set local-traffic [enable|disable]
  set multicast-traffic [enable|disable]
```

```

set severity [emergency|alert|...]
set sniffer-traffic [enable|disable]
set voip [enable|disable]
set ztna-traffic [enable|disable]
end

```

## config log fortianalyzer-cloud filter

Parameter	Description	Type	Size	Default						
anomaly	Enable/disable anomaly logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable anomaly logging.</td></tr><tr><td><i>disable</i></td><td>Disable anomaly logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable anomaly logging.	<i>disable</i>	Disable anomaly logging.			
Option	Description									
<i>enable</i>	Enable anomaly logging.									
<i>disable</i>	Disable anomaly logging.									
dlp-archive	Enable/disable DLP archive logging.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable DLP archive logging.</td></tr><tr><td><i>disable</i></td><td>Disable DLP archive logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable DLP archive logging.	<i>disable</i>	Disable DLP archive logging.			
Option	Description									
<i>enable</i>	Enable DLP archive logging.									
<i>disable</i>	Disable DLP archive logging.									
forward-traffic	Enable/disable forward traffic logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable forward traffic logging.</td></tr><tr><td><i>disable</i></td><td>Disable forward traffic logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable forward traffic logging.	<i>disable</i>	Disable forward traffic logging.			
Option	Description									
<i>enable</i>	Enable forward traffic logging.									
<i>disable</i>	Disable forward traffic logging.									
gtp *	Enable/disable GTP messages logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable GTP messages logging.</td></tr><tr><td><i>disable</i></td><td>Disable GTP messages logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable GTP messages logging.	<i>disable</i>	Disable GTP messages logging.			
Option	Description									
<i>enable</i>	Enable GTP messages logging.									
<i>disable</i>	Disable GTP messages logging.									
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable local in or out traffic logging.</td></tr><tr><td><i>disable</i></td><td>Disable local in or out traffic logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable local in or out traffic logging.	<i>disable</i>	Disable local in or out traffic logging.			
Option	Description									
<i>enable</i>	Enable local in or out traffic logging.									
<i>disable</i>	Disable local in or out traffic logging.									
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable						

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable multicast traffic logging.		
	<i>disable</i>	Disable multicast traffic logging.		
severity	Lowest severity level to log.	option	-	information
	<b>Option</b>	<b>Description</b>		
	<i>emergency</i>	Emergency level.		
	<i>alert</i>	Alert level.		
	<i>critical</i>	Critical level.		
	<i>error</i>	Error level.		
	<i>warning</i>	Warning level.		
	<i>notification</i>	Notification level.		
	<i>information</i>	Information level.		
	<i>debug</i>	Debug level.		
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable sniffer traffic logging.		
	<i>disable</i>	Disable sniffer traffic logging.		
voip	Enable/disable VoIP logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable VoIP logging.		
	<i>disable</i>	Disable VoIP logging.		
ztna-traffic	Enable/disable ztna traffic logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable ztna traffic logging.		
	<i>disable</i>	Disable ztna traffic logging.		

\* This parameter may not exist in some models.

## config free-style

Parameter	Description	Type	Size	Default																																		
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0																																		
category	Log category.	option	-	traffic																																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>traffic</td><td>Traffic log.</td></tr><tr><td>event</td><td>Event log.</td></tr><tr><td>virus</td><td>Antivirus log.</td></tr><tr><td>webfilter</td><td>Web filter log.</td></tr><tr><td>attack</td><td>Attack log.</td></tr><tr><td>spam</td><td>Antispam log.</td></tr><tr><td>anomaly</td><td>Anomaly log.</td></tr><tr><td>voip</td><td>VoIP log.</td></tr><tr><td>dlp</td><td>DLP log.</td></tr><tr><td>app-ctrl</td><td>Application control log.</td></tr><tr><td>waf</td><td>Web application firewall log.</td></tr><tr><td>dns</td><td>DNS detail log.</td></tr><tr><td>ssh</td><td>SSH log.</td></tr><tr><td>ssl</td><td>SSL log.</td></tr><tr><td>file-filter</td><td>File filter log.</td></tr><tr><td>icap</td><td>ICAP log.</td></tr></table>	Option	Description	traffic	Traffic log.	event	Event log.	virus	Antivirus log.	webfilter	Web filter log.	attack	Attack log.	spam	Antispam log.	anomaly	Anomaly log.	voip	VoIP log.	dlp	DLP log.	app-ctrl	Application control log.	waf	Web application firewall log.	dns	DNS detail log.	ssh	SSH log.	ssl	SSL log.	file-filter	File filter log.	icap	ICAP log.			
	Option	Description																																				
	traffic	Traffic log.																																				
	event	Event log.																																				
	virus	Antivirus log.																																				
	webfilter	Web filter log.																																				
	attack	Attack log.																																				
	spam	Antispam log.																																				
	anomaly	Anomaly log.																																				
	voip	VoIP log.																																				
	dlp	DLP log.																																				
	app-ctrl	Application control log.																																				
	waf	Web application firewall log.																																				
	dns	DNS detail log.																																				
	ssh	SSH log.																																				
	ssl	SSL log.																																				
file-filter	File filter log.																																					
icap	ICAP log.																																					
filter	Free style filter string.	string	Maximum length: 1023																																			
filter-type	Include/exclude logs that match the filter.	option	-	include																																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>include</td><td>Include logs that match the filter.</td></tr><tr><td>exclude</td><td>Exclude logs that match the filter.</td></tr></table>	Option	Description	include	Include logs that match the filter.	exclude	Exclude logs that match the filter.																															
	Option	Description																																				
	include	Include logs that match the filter.																																				
exclude	Exclude logs that match the filter.																																					

## config log fortianalyzer-cloud override-filter

Override filters for FortiAnalyzer Cloud.

```
config log fortianalyzer-cloud override-filter
  Description: Override filters for FortiAnalyzer Cloud.
  set anomaly [enable|disable]
  set dlp-archive [enable|disable]
  set forward-traffic [enable|disable]
  config free-style
    Description: Free style filters.
    edit <id>
      set category [traffic|event|...]
      set filter {string}
      set filter-type [include|exclude]
    next
  end
  set gtp [enable|disable]
  set local-traffic [enable|disable]
  set multicast-traffic [enable|disable]
  set severity [emergency|alert|...]
  set sniffer-traffic [enable|disable]
  set voip [enable|disable]
  set ztna-traffic [enable|disable]
end
```

## config log fortianalyzer-cloud override-filter

Parameter	Description	Type	Size	Default
anomaly	Enable/disable anomaly logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable anomaly logging.		
	<i>disable</i>	Disable anomaly logging.		
dlp-archive	Enable/disable DLP archive logging.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable DLP archive logging.		
	<i>disable</i>	Disable DLP archive logging.		
forward-traffic	Enable/disable forward traffic logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable forward traffic logging.		
	<i>disable</i>	Disable forward traffic logging.		

Parameter	Description	Type	Size	Default																		
gtp *	Enable/disable GTP messages logging.	option	-	enable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable GTP messages logging.</td></tr><tr><td><i>disable</i></td><td>Disable GTP messages logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable GTP messages logging.	<i>disable</i>	Disable GTP messages logging.															
Option	Description																					
<i>enable</i>	Enable GTP messages logging.																					
<i>disable</i>	Disable GTP messages logging.																					
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable local in or out traffic logging.</td></tr><tr><td><i>disable</i></td><td>Disable local in or out traffic logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable local in or out traffic logging.	<i>disable</i>	Disable local in or out traffic logging.															
Option	Description																					
<i>enable</i>	Enable local in or out traffic logging.																					
<i>disable</i>	Disable local in or out traffic logging.																					
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable multicast traffic logging.</td></tr><tr><td><i>disable</i></td><td>Disable multicast traffic logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable multicast traffic logging.	<i>disable</i>	Disable multicast traffic logging.															
Option	Description																					
<i>enable</i>	Enable multicast traffic logging.																					
<i>disable</i>	Disable multicast traffic logging.																					
severity	Lowest severity level to log.	option	-	information																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>emergency</i></td><td>Emergency level.</td></tr><tr><td><i>alert</i></td><td>Alert level.</td></tr><tr><td><i>critical</i></td><td>Critical level.</td></tr><tr><td><i>error</i></td><td>Error level.</td></tr><tr><td><i>warning</i></td><td>Warning level.</td></tr><tr><td><i>notification</i></td><td>Notification level.</td></tr><tr><td><i>information</i></td><td>Information level.</td></tr><tr><td><i>debug</i></td><td>Debug level.</td></tr></table>	Option	Description	<i>emergency</i>	Emergency level.	<i>alert</i>	Alert level.	<i>critical</i>	Critical level.	<i>error</i>	Error level.	<i>warning</i>	Warning level.	<i>notification</i>	Notification level.	<i>information</i>	Information level.	<i>debug</i>	Debug level.			
Option	Description																					
<i>emergency</i>	Emergency level.																					
<i>alert</i>	Alert level.																					
<i>critical</i>	Critical level.																					
<i>error</i>	Error level.																					
<i>warning</i>	Warning level.																					
<i>notification</i>	Notification level.																					
<i>information</i>	Information level.																					
<i>debug</i>	Debug level.																					
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable sniffer traffic logging.</td></tr><tr><td><i>disable</i></td><td>Disable sniffer traffic logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable sniffer traffic logging.	<i>disable</i>	Disable sniffer traffic logging.															
Option	Description																					
<i>enable</i>	Enable sniffer traffic logging.																					
<i>disable</i>	Disable sniffer traffic logging.																					
voip	Enable/disable VoIP logging.	option	-	enable																		

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable VoIP logging.		
	<i>disable</i>	Disable VoIP logging.		
ztna-traffic	Enable/disable ztna traffic logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable ztna traffic logging.		
	<i>disable</i>	Disable ztna traffic logging.		

\* This parameter may not exist in some models.

### config free-style

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
category	Log category.	option	-	traffic
	<b>Option</b>	<b>Description</b>		
	<i>traffic</i>	Traffic log.		
	<i>event</i>	Event log.		
	<i>virus</i>	Antivirus log.		
	<i>webfilter</i>	Web filter log.		
	<i>attack</i>	Attack log.		
	<i>spam</i>	Antispam log.		
	<i>anomaly</i>	Anomaly log.		
	<i>voip</i>	VoIP log.		
	<i>dlp</i>	DLP log.		
	<i>app-ctrl</i>	Application control log.		
	<i>waf</i>	Web application firewall log.		
	<i>dns</i>	DNS detail log.		



Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>ssh</i>	SSH log.		
	<i>ssl</i>	SSL log.		
	<i>file-filter</i>	File filter log.		
	<i>icap</i>	ICAP log.		
filter	Free style filter string.	string	Maximum length: 1023	
filter-type	Include/exclude logs that match the filter.	option	-	include
	<b>Option</b>	<b>Description</b>		
	<i>include</i>	Include logs that match the filter.		
	<i>exclude</i>	Exclude logs that match the filter.		

## config log fortianalyzer-cloud override-setting

Override FortiAnalyzer Cloud settings.

```
config log fortianalyzer-cloud override-setting
    Description: Override FortiAnalyzer Cloud settings.
    set status [enable|disable]
end
```

## config log fortianalyzer-cloud override-setting

Parameter	Description	Type	Size	Default
status	Enable/disable logging to FortiAnalyzer.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable logging to FortiAnalyzer.		
	<i>disable</i>	Disable logging to FortiAnalyzer.		

## config log fortianalyzer-cloud setting

Global FortiAnalyzer Cloud settings.

```
config log fortianalyzer-cloud setting
    Description: Global FortiAnalyzer Cloud settings.
    set access-config [enable|disable]
    set certificate {string}
```

```

set certificate-verification [enable|disable]
set conn-timeout {integer}
set enc-algorithm [high-medium|high|...]
set hmac-algorithm [sha256|sha1]
set interface {string}
set interface-select-method [auto|sdwan|...]
set ips-archive [enable|disable]
set max-log-rate {integer}
set monitor-failure-retry-period {integer}
set monitor-keepalive-period {integer}
set preshared-key {string}
set priority [default|low]
set serial <name1>, <name2>, ...
set source-ip {string}
set ssl-min-proto-version [default|SSLv3|...]
set status [enable|disable]
set upload-day {user}
set upload-interval [daily|weekly|...]
set upload-option [store-and-upload|realtime|...]
set upload-time {user}

```

end

## config log fortianalyzer-cloud setting

Parameter	Description	Type	Size	Default						
access-config	Enable/disable FortiAnalyzer access to configuration and data.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable FortiAnalyzer access to configuration and data.</td></tr><tr><td><i>disable</i></td><td>Disable FortiAnalyzer access to configuration and data.</td></tr></table>	Option	Description	<i>enable</i>	Enable FortiAnalyzer access to configuration and data.	<i>disable</i>	Disable FortiAnalyzer access to configuration and data.			
Option	Description									
<i>enable</i>	Enable FortiAnalyzer access to configuration and data.									
<i>disable</i>	Disable FortiAnalyzer access to configuration and data.									
certificate	Certificate used to communicate with FortiAnalyzer.	string	Maximum length: 35							
certificate-verification	Enable/disable identity verification of FortiAnalyzer by use of certificate.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable identity verification of FortiAnalyzer by use of certificate.</td></tr><tr><td><i>disable</i></td><td>Disable identity verification of FortiAnalyzer by use of certificate.</td></tr></table>	Option	Description	<i>enable</i>	Enable identity verification of FortiAnalyzer by use of certificate.	<i>disable</i>	Disable identity verification of FortiAnalyzer by use of certificate.			
Option	Description									
<i>enable</i>	Enable identity verification of FortiAnalyzer by use of certificate.									
<i>disable</i>	Disable identity verification of FortiAnalyzer by use of certificate.									
conn-timeout	FortiAnalyzer connection time-out in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 3600	10						
enc-algorithm	Configure the level of SSL protection for secure communication with FortiAnalyzer.	option	-	high						

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>high-medium</i></td><td>Encrypt logs using high and medium encryption algorithms.</td></tr><tr><td><i>high</i></td><td>Encrypt logs using high encryption algorithms.</td></tr><tr><td><i>low</i></td><td>Encrypt logs using all encryption algorithms.</td></tr></table>	Option	Description	<i>high-medium</i>	Encrypt logs using high and medium encryption algorithms.	<i>high</i>	Encrypt logs using high encryption algorithms.	<i>low</i>	Encrypt logs using all encryption algorithms.			
	Option	Description										
	<i>high-medium</i>	Encrypt logs using high and medium encryption algorithms.										
	<i>high</i>	Encrypt logs using high encryption algorithms.										
<i>low</i>	Encrypt logs using all encryption algorithms.											
hmac-algorithm	FortiAnalyzer IPsec tunnel HMAC algorithm.	option	-	sha256								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>sha256</i></td><td>Use SHA256 as HMAC algorithm.</td></tr><tr><td><i>sha1</i></td><td>Step down to SHA1 as the HMAC algorithm.</td></tr></table>	Option	Description	<i>sha256</i>	Use SHA256 as HMAC algorithm.	<i>sha1</i>	Step down to SHA1 as the HMAC algorithm.					
	Option	Description										
	<i>sha256</i>	Use SHA256 as HMAC algorithm.										
<i>sha1</i>	Step down to SHA1 as the HMAC algorithm.											
interface	Specify outgoing interface to reach server.	string	Maximum length: 15									
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto</i></td><td>Set outgoing interface automatically.</td></tr><tr><td><i>sdwan</i></td><td>Set outgoing interface by SD-WAN or policy routing rules.</td></tr><tr><td><i>specify</i></td><td>Set outgoing interface manually.</td></tr></table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.			
	Option	Description										
	<i>auto</i>	Set outgoing interface automatically.										
	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.										
<i>specify</i>	Set outgoing interface manually.											
ips-archive	Enable/disable IPS packet archive logging.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable IPS packet archive logging.</td></tr><tr><td><i>disable</i></td><td>Disable IPS packet archive logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable IPS packet archive logging.	<i>disable</i>	Disable IPS packet archive logging.					
	Option	Description										
	<i>enable</i>	Enable IPS packet archive logging.										
<i>disable</i>	Disable IPS packet archive logging.											
max-log-rate	FortiAnalyzer maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0								
monitor-failure-retry-period	Time between FortiAnalyzer connection retries in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 86400	5								

Parameter	Description	Type	Size	Default												
monitor-keepalive-period	Time between OFTP keepalives in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 120	5												
preshared-key	Preshared-key used for auto-authorization on FortiAnalyzer.	string	Maximum length: 63													
priority	Set log transmission priority.	option	-	default												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>default</td><td>Set FortiAnalyzer log transmission priority to default.</td></tr><tr><td>low</td><td>Set FortiAnalyzer log transmission priority to low.</td></tr></table>				Option	Description	default	Set FortiAnalyzer log transmission priority to default.	low	Set FortiAnalyzer log transmission priority to low.						
Option	Description															
default	Set FortiAnalyzer log transmission priority to default.															
low	Set FortiAnalyzer log transmission priority to low.															
serial <name>	Serial numbers of the FortiAnalyzer. Serial Number.	string	Maximum length: 79													
source-ip	Source IPv4 or IPv6 address used to communicate with FortiAnalyzer.	string	Maximum length: 63													
ssl-min-protocol-version	Minimum supported protocol version for SSL/TLS connections.	option	-	default												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>default</td><td>Follow system global setting.</td></tr><tr><td>SSLv3</td><td>SSLv3.</td></tr><tr><td>TLSv1</td><td>TLSv1.</td></tr><tr><td>TLSv1-1</td><td>TLSv1.1.</td></tr><tr><td>TLSv1-2</td><td>TLSv1.2.</td></tr></table>				Option	Description	default	Follow system global setting.	SSLv3	SSLv3.	TLSv1	TLSv1.	TLSv1-1	TLSv1.1.	TLSv1-2	TLSv1.2.
Option	Description															
default	Follow system global setting.															
SSLv3	SSLv3.															
TLSv1	TLSv1.															
TLSv1-1	TLSv1.1.															
TLSv1-2	TLSv1.2.															
status	Enable/disable logging to FortiAnalyzer.	option	-	disable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable logging to FortiAnalyzer.</td></tr><tr><td>disable</td><td>Disable logging to FortiAnalyzer.</td></tr></table>				Option	Description	enable	Enable logging to FortiAnalyzer.	disable	Disable logging to FortiAnalyzer.						
Option	Description															
enable	Enable logging to FortiAnalyzer.															
disable	Disable logging to FortiAnalyzer.															
upload-day	Day of week (month) to upload logs.	user	Not Specified													
upload-interval	Frequency to upload log files to FortiAnalyzer.	option	-	daily												

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>daily</i>	Upload log files to FortiAnalyzer once a day.		
	<i>weekly</i>	Upload log files to FortiAnalyzer once a week.		
	<i>monthly</i>	Upload log files to FortiAnalyzer once a month.		
upload-option	Enable/disable logging to hard disk and then uploading to FortiAnalyzer.	option	-	5-minute
	<b>Option</b>	<b>Description</b>		
	<i>store-and-upload</i>	Log to hard disk and then upload to FortiAnalyzer.		
	<i>realtime</i>	Log directly to FortiAnalyzer in real time.		
	<i>1-minute</i>	Log directly to FortiAnalyzer at least every 1 minute.		
	<i>5-minute</i>	Log directly to FortiAnalyzer at least every 5 minutes.		
upload-time	Time to upload logs (hh:mm).	user	Not Specified	

## config log fortianalyzer2 filter

Filters for FortiAnalyzer.

```

config log fortianalyzer2 filter
    Description: Filters for FortiAnalyzer.
    set anomaly [enable|disable]
    set dlp-archive [enable|disable]
    set forward-traffic [enable|disable]
    config free-style
        Description: Free style filters.
        edit <id>
            set category [traffic|event|...]
            set filter {string}
            set filter-type [include|exclude]
        next
    end
    set gtp [enable|disable]
    set local-traffic [enable|disable]
    set multicast-traffic [enable|disable]
    set severity [emergency|alert|...]
    set sniffer-traffic [enable|disable]
    set voip [enable|disable]
    set ztna-traffic [enable|disable]
end

```

## config log fortianalyzer2 filter

Parameter	Description	Type	Size	Default
anomaly	Enable/disable anomaly logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable anomaly logging.		
	<i>disable</i>	Disable anomaly logging.		
dlp-archive	Enable/disable DLP archive logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable DLP archive logging.		
	<i>disable</i>	Disable DLP archive logging.		
forward-traffic	Enable/disable forward traffic logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable forward traffic logging.		
	<i>disable</i>	Disable forward traffic logging.		
gtp *	Enable/disable GTP messages logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable GTP messages logging.		
	<i>disable</i>	Disable GTP messages logging.		
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable local in or out traffic logging.		
	<i>disable</i>	Disable local in or out traffic logging.		
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable multicast traffic logging.		
	<i>disable</i>	Disable multicast traffic logging.		
severity	Log every message above and including this severity level.	option	-	information

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>emergency</i>	Emergency level.		
	<i>alert</i>	Alert level.		
	<i>critical</i>	Critical level.		
	<i>error</i>	Error level.		
	<i>warning</i>	Warning level.		
	<i>notification</i>	Notification level.		
	<i>information</i>	Information level.		
	<i>debug</i>	Debug level.		
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable sniffer traffic logging.		
	<i>disable</i>	Disable sniffer traffic logging.		
voip	Enable/disable VoIP logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable VoIP logging.		
	<i>disable</i>	Disable VoIP logging.		
ztna-traffic	Enable/disable ztna traffic logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable ztna traffic logging.		
	<i>disable</i>	Disable ztna traffic logging.		

\* This parameter may not exist in some models.

### config free-style

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0

Parameter	Description	Type	Size	Default																																			
category	Log category.	option	-	traffic																																			
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>traffic</td><td>Traffic log.</td></tr><tr><td>event</td><td>Event log.</td></tr><tr><td>virus</td><td>Antivirus log.</td></tr><tr><td>webfilter</td><td>Web filter log.</td></tr><tr><td>attack</td><td>Attack log.</td></tr><tr><td>spam</td><td>Antispam log.</td></tr><tr><td>anomaly</td><td>Anomaly log.</td></tr><tr><td>voip</td><td>VoIP log.</td></tr><tr><td>dlp</td><td>DLP log.</td></tr><tr><td>app-ctrl</td><td>Application control log.</td></tr><tr><td>waf</td><td>Web application firewall log.</td></tr><tr><td>dns</td><td>DNS detail log.</td></tr><tr><td>ssh</td><td>SSH log.</td></tr><tr><td>ssl</td><td>SSL log.</td></tr><tr><td>file-filter</td><td>File filter log.</td></tr><tr><td>icap</td><td>ICAP log.</td></tr></table>	Option	Description	traffic	Traffic log.	event	Event log.	virus	Antivirus log.	webfilter	Web filter log.	attack	Attack log.	spam	Antispam log.	anomaly	Anomaly log.	voip	VoIP log.	dlp	DLP log.	app-ctrl	Application control log.	waf	Web application firewall log.	dns	DNS detail log.	ssh	SSH log.	ssl	SSL log.	file-filter	File filter log.	icap	ICAP log.				
	Option	Description																																					
	traffic	Traffic log.																																					
	event	Event log.																																					
	virus	Antivirus log.																																					
	webfilter	Web filter log.																																					
	attack	Attack log.																																					
	spam	Antispam log.																																					
	anomaly	Anomaly log.																																					
	voip	VoIP log.																																					
	dlp	DLP log.																																					
	app-ctrl	Application control log.																																					
	waf	Web application firewall log.																																					
	dns	DNS detail log.																																					
	ssh	SSH log.																																					
	ssl	SSL log.																																					
	file-filter	File filter log.																																					
icap	ICAP log.																																						
filter	Free style filter string.	string	Maximum length: 1023																																				
filter-type	Include/exclude logs that match the filter.	option	-	include																																			
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>include</td><td>Include logs that match the filter.</td></tr><tr><td>exclude</td><td>Exclude logs that match the filter.</td></tr></table>	Option	Description	include	Include logs that match the filter.	exclude	Exclude logs that match the filter.																																
	Option	Description																																					
	include	Include logs that match the filter.																																					
exclude	Exclude logs that match the filter.																																						

### config log fortianalyzer2 override-filter

Override filters for FortiAnalyzer.

```
config log fortianalyzer2 override-filter
  Description: Override filters for FortiAnalyzer.
  set anomaly [enable|disable]
  set dlp-archive [enable|disable]
  set forward-traffic [enable|disable]
  config free-style
```



```

Description: Free style filters.
edit <id>
    set category [traffic|event|...]
    set filter {string}
    set filter-type [include|exclude]
next
end
set gtp [enable|disable]
set local-traffic [enable|disable]
set multicast-traffic [enable|disable]
set severity [emergency|alert|...]
set sniffer-traffic [enable|disable]
set voip [enable|disable]
set ztna-traffic [enable|disable]
end

```

## config log fortianalyzer2 override-filter

Parameter	Description	Type	Size	Default
anomaly	Enable/disable anomaly logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable anomaly logging.		
	<i>disable</i>	Disable anomaly logging.		
dlp-archive	Enable/disable DLP archive logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable DLP archive logging.		
	<i>disable</i>	Disable DLP archive logging.		
forward-traffic	Enable/disable forward traffic logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable forward traffic logging.		
	<i>disable</i>	Disable forward traffic logging.		
gtp *	Enable/disable GTP messages logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable GTP messages logging.		
	<i>disable</i>	Disable GTP messages logging.		
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable local in or out traffic logging.		
	<i>disable</i>	Disable local in or out traffic logging.		
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable multicast traffic logging.		
	<i>disable</i>	Disable multicast traffic logging.		
severity	Log every message above and including this severity level.	option	-	information
	<b>Option</b>	<b>Description</b>		
	<i>emergency</i>	Emergency level.		
	<i>alert</i>	Alert level.		
	<i>critical</i>	Critical level.		
	<i>error</i>	Error level.		
	<i>warning</i>	Warning level.		
	<i>notification</i>	Notification level.		
	<i>information</i>	Information level.		
	<i>debug</i>	Debug level.		
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable sniffer traffic logging.		
	<i>disable</i>	Disable sniffer traffic logging.		
voip	Enable/disable VoIP logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable VoIP logging.		
	<i>disable</i>	Disable VoIP logging.		
ztina-traffic	Enable/disable ztna traffic logging.	option	-	enable

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable ztna traffic logging.		
	<i>disable</i>	Disable ztna traffic logging.		

\* This parameter may not exist in some models.

### config free-style

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
category	Log category.	option	-	traffic
	<b>Option</b>	<b>Description</b>		
	<i>traffic</i>	Traffic log.		
	<i>event</i>	Event log.		
	<i>virus</i>	Antivirus log.		
	<i>webfilter</i>	Web filter log.		
	<i>attack</i>	Attack log.		
	<i>spam</i>	Antispam log.		
	<i>anomaly</i>	Anomaly log.		
	<i>voip</i>	VoIP log.		
	<i>dlp</i>	DLP log.		
	<i>app-ctrl</i>	Application control log.		
	<i>waf</i>	Web application firewall log.		
	<i>dns</i>	DNS detail log.		
	<i>ssh</i>	SSH log.		
	<i>ssl</i>	SSL log.		
	<i>file-filter</i>	File filter log.		
	<i>icap</i>	ICAP log.		

Parameter	Description	Type	Size	Default						
filter	Free style filter string.	string	Maximum length: 1023							
filter-type	Include/exclude logs that match the filter.	option	-	include						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>include</i></td><td>Include logs that match the filter.</td></tr><tr><td><i>exclude</i></td><td>Exclude logs that match the filter.</td></tr></table>				Option	Description	<i>include</i>	Include logs that match the filter.	<i>exclude</i>	Exclude logs that match the filter.
Option	Description									
<i>include</i>	Include logs that match the filter.									
<i>exclude</i>	Exclude logs that match the filter.									

## config log fortianalyzer2 override-setting

Override FortiAnalyzer settings.

```
config log fortianalyzer2 override-setting
    Description: Override FortiAnalyzer settings.
    set access-config [enable|disable]
    set certificate {string}
    set certificate-verification [enable|disable]
    set conn-timeout {integer}
    set enc-algorithm [high-medium|high|...]
    set hmac-algorithm [sha256|sha1]
    set interface {string}
    set interface-select-method [auto|sdwan|...]
    set ips-archive [enable|disable]
    set max-log-rate {integer}
    set monitor-failure-retry-period {integer}
    set monitor-keepalive-period {integer}
    set preshared-key {string}
    set priority [default|low]
    set reliable [enable|disable]
    set serial <name1>, <name2>, ...
    set server {string}
    set source-ip {string}
    set ssl-min-proto-version [default|SSLv3|...]
    set status [enable|disable]
    set upload-day {user}
    set upload-interval [daily|weekly|...]
    set upload-option [store-and-upload|realtime|...]
    set upload-time {user}
    set use-management-vdom [enable|disable]
end
```

## config log fortianalyzer2 override-setting

Parameter	Description	Type	Size	Default
access-config	Enable/disable FortiAnalyzer access to configuration and data.	option	-	enable

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable FortiAnalyzer access to configuration and data.</td></tr><tr><td><i>disable</i></td><td>Disable FortiAnalyzer access to configuration and data.</td></tr></table>	Option	Description	<i>enable</i>	Enable FortiAnalyzer access to configuration and data.	<i>disable</i>	Disable FortiAnalyzer access to configuration and data.					
Option	Description											
<i>enable</i>	Enable FortiAnalyzer access to configuration and data.											
<i>disable</i>	Disable FortiAnalyzer access to configuration and data.											
certificate	Certificate used to communicate with FortiAnalyzer.	string	Maximum length: 35									
certificate-verification	Enable/disable identity verification of FortiAnalyzer by use of certificate.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable identity verification of FortiAnalyzer by use of certificate.</td></tr><tr><td><i>disable</i></td><td>Disable identity verification of FortiAnalyzer by use of certificate.</td></tr></table>	Option	Description	<i>enable</i>	Enable identity verification of FortiAnalyzer by use of certificate.	<i>disable</i>	Disable identity verification of FortiAnalyzer by use of certificate.					
Option	Description											
<i>enable</i>	Enable identity verification of FortiAnalyzer by use of certificate.											
<i>disable</i>	Disable identity verification of FortiAnalyzer by use of certificate.											
conn-timeout	FortiAnalyzer connection time-out in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 3600	10								
enc-algorithm	Configure the level of SSL protection for secure communication with FortiAnalyzer.	option	-	high								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>high-medium</i></td><td>Encrypt logs using high and medium encryption algorithms.</td></tr><tr><td><i>high</i></td><td>Encrypt logs using high encryption algorithms.</td></tr><tr><td><i>low</i></td><td>Encrypt logs using all encryption algorithms.</td></tr></table>	Option	Description	<i>high-medium</i>	Encrypt logs using high and medium encryption algorithms.	<i>high</i>	Encrypt logs using high encryption algorithms.	<i>low</i>	Encrypt logs using all encryption algorithms.			
Option	Description											
<i>high-medium</i>	Encrypt logs using high and medium encryption algorithms.											
<i>high</i>	Encrypt logs using high encryption algorithms.											
<i>low</i>	Encrypt logs using all encryption algorithms.											
hmac-algorithm	FortiAnalyzer IPsec tunnel HMAC algorithm.	option	-	sha256								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>sha256</i></td><td>Use SHA256 as HMAC algorithm.</td></tr><tr><td><i>sha1</i></td><td>Step down to SHA1 as the HMAC algorithm.</td></tr></table>	Option	Description	<i>sha256</i>	Use SHA256 as HMAC algorithm.	<i>sha1</i>	Step down to SHA1 as the HMAC algorithm.					
Option	Description											
<i>sha256</i>	Use SHA256 as HMAC algorithm.											
<i>sha1</i>	Step down to SHA1 as the HMAC algorithm.											
interface	Specify outgoing interface to reach server.	string	Maximum length: 15									
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto</i></td><td>Set outgoing interface automatically.</td></tr></table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.							
Option	Description											
<i>auto</i>	Set outgoing interface automatically.											

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>sdwan</i></td><td>Set outgoing interface by SD-WAN or policy routing rules.</td></tr><tr><td><i>specify</i></td><td>Set outgoing interface manually.</td></tr></table>	Option	Description	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.			
	Option	Description								
	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.								
<i>specify</i>	Set outgoing interface manually.									
ips-archive	Enable/disable IPS packet archive logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable IPS packet archive logging.</td></tr><tr><td><i>disable</i></td><td>Disable IPS packet archive logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable IPS packet archive logging.	<i>disable</i>	Disable IPS packet archive logging.			
	Option	Description								
	<i>enable</i>	Enable IPS packet archive logging.								
<i>disable</i>	Disable IPS packet archive logging.									
max-log-rate	FortiAnalyzer maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0						
monitor-failure-retry-period	Time between FortiAnalyzer connection retries in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 86400	5						
monitor-keepalive-period	Time between OFTP keepalives in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 120	5						
preshared-key	Preshared-key used for auto-authorization on FortiAnalyzer.	string	Maximum length: 63							
priority	Set log transmission priority.	option	-	default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>Set FortiAnalyzer log transmission priority to default.</td></tr><tr><td><i>low</i></td><td>Set FortiAnalyzer log transmission priority to low.</td></tr></table>	Option	Description	<i>default</i>	Set FortiAnalyzer log transmission priority to default.	<i>low</i>	Set FortiAnalyzer log transmission priority to low.			
	Option	Description								
	<i>default</i>	Set FortiAnalyzer log transmission priority to default.								
<i>low</i>	Set FortiAnalyzer log transmission priority to low.									
reliable	Enable/disable reliable logging to FortiAnalyzer.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable reliable logging to FortiAnalyzer.</td></tr><tr><td><i>disable</i></td><td>Disable reliable logging to FortiAnalyzer.</td></tr></table>	Option	Description	<i>enable</i>	Enable reliable logging to FortiAnalyzer.	<i>disable</i>	Disable reliable logging to FortiAnalyzer.			
	Option	Description								
	<i>enable</i>	Enable reliable logging to FortiAnalyzer.								
<i>disable</i>	Disable reliable logging to FortiAnalyzer.									
serial <name>	Serial numbers of the FortiAnalyzer. Serial Number.	string	Maximum length: 79							

Parameter	Description	Type	Size	Default												
server	The remote FortiAnalyzer.	string	Maximum length: 127													
source-ip	Source IPv4 or IPv6 address used to communicate with FortiAnalyzer.	string	Maximum length: 63													
ssl-min-protocol-version	Minimum supported protocol version for SSL/TLS connections.	option	-	default												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>default</td><td>Follow system global setting.</td></tr><tr><td>SSLv3</td><td>SSLv3.</td></tr><tr><td>TLSv1</td><td>TLSv1.</td></tr><tr><td>TLSv1-1</td><td>TLSv1.1.</td></tr><tr><td>TLSv1-2</td><td>TLSv1.2.</td></tr></table>	Option	Description	default	Follow system global setting.	SSLv3	SSLv3.	TLSv1	TLSv1.	TLSv1-1	TLSv1.1.	TLSv1-2	TLSv1.2.			
Option	Description															
default	Follow system global setting.															
SSLv3	SSLv3.															
TLSv1	TLSv1.															
TLSv1-1	TLSv1.1.															
TLSv1-2	TLSv1.2.															
status	Enable/disable logging to FortiAnalyzer.	option	-	disable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable logging to FortiAnalyzer.</td></tr><tr><td>disable</td><td>Disable logging to FortiAnalyzer.</td></tr></table>	Option	Description	enable	Enable logging to FortiAnalyzer.	disable	Disable logging to FortiAnalyzer.									
Option	Description															
enable	Enable logging to FortiAnalyzer.															
disable	Disable logging to FortiAnalyzer.															
upload-day	Day of week (month) to upload logs.	user	Not Specified													
upload-interval	Frequency to upload log files to FortiAnalyzer.	option	-	daily												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>daily</td><td>Upload log files to FortiAnalyzer once a day.</td></tr><tr><td>weekly</td><td>Upload log files to FortiAnalyzer once a week.</td></tr><tr><td>monthly</td><td>Upload log files to FortiAnalyzer once a month.</td></tr></table>	Option	Description	daily	Upload log files to FortiAnalyzer once a day.	weekly	Upload log files to FortiAnalyzer once a week.	monthly	Upload log files to FortiAnalyzer once a month.							
Option	Description															
daily	Upload log files to FortiAnalyzer once a day.															
weekly	Upload log files to FortiAnalyzer once a week.															
monthly	Upload log files to FortiAnalyzer once a month.															
upload-option	Enable/disable logging to hard disk and then uploading to FortiAnalyzer.	option	-	5-minute												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>store-and-upload</td><td>Log to hard disk and then upload to FortiAnalyzer.</td></tr><tr><td>realtime</td><td>Log directly to FortiAnalyzer in real time.</td></tr><tr><td>1-minute</td><td>Log directly to FortiAnalyzer at least every 1 minute.</td></tr><tr><td>5-minute</td><td>Log directly to FortiAnalyzer at least every 5 minutes.</td></tr></table>	Option	Description	store-and-upload	Log to hard disk and then upload to FortiAnalyzer.	realtime	Log directly to FortiAnalyzer in real time.	1-minute	Log directly to FortiAnalyzer at least every 1 minute.	5-minute	Log directly to FortiAnalyzer at least every 5 minutes.					
Option	Description															
store-and-upload	Log to hard disk and then upload to FortiAnalyzer.															
realtime	Log directly to FortiAnalyzer in real time.															
1-minute	Log directly to FortiAnalyzer at least every 1 minute.															
5-minute	Log directly to FortiAnalyzer at least every 5 minutes.															

Parameter	Description	Type	Size	Default
upload-time	Time to upload logs (hh:mm).	user	Not Specified	
use-management-vdom	Enable/disable use of management VDOM IP address as source IP for logs sent to FortiAnalyzer.	option	-	disable
		Option	Description	
		<i>enable</i>	Enable use of management VDOM IP address as source IP for logs sent to FortiAnalyzer.	
		<i>disable</i>	Disable use of management VDOM IP address as source IP for logs sent to FortiAnalyzer.	

## config log fortianalyzer2 setting

Global FortiAnalyzer settings.

```
config log fortianalyzer2 setting
    Description: Global FortiAnalyzer settings.
    set access-config [enable|disable]
    set certificate {string}
    set certificate-verification [enable|disable]
    set conn-timeout {integer}
    set enc-algorithm [high-medium|high|...]
    set hmac-algorithm [sha256|sha1]
    set interface {string}
    set interface-select-method [auto|sdwan|...]
    set ips-archive [enable|disable]
    set max-log-rate {integer}
    set monitor-failure-retry-period {integer}
    set monitor-keepalive-period {integer}
    set preshared-key {string}
    set priority [default|low]
    set reliable [enable|disable]
    set serial <name1>, <name2>, ...
    set server {string}
    set source-ip {string}
    set ssl-min-proto-version [default|SSLv3|...]
    set status [enable|disable]
    set upload-day {user}
    set upload-interval [daily|weekly|...]
    set upload-option [store-and-upload|realtime|...]
    set upload-time {user}
end
```



## config log fortianalyzer2 setting

Parameter	Description	Type	Size	Default								
access-config	Enable/disable FortiAnalyzer access to configuration and data.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable FortiAnalyzer access to configuration and data.</td></tr><tr><td><i>disable</i></td><td>Disable FortiAnalyzer access to configuration and data.</td></tr></table>	Option	Description	<i>enable</i>	Enable FortiAnalyzer access to configuration and data.	<i>disable</i>	Disable FortiAnalyzer access to configuration and data.					
Option	Description											
<i>enable</i>	Enable FortiAnalyzer access to configuration and data.											
<i>disable</i>	Disable FortiAnalyzer access to configuration and data.											
certificate	Certificate used to communicate with FortiAnalyzer.	string	Maximum length: 35									
certificate-verification	Enable/disable identity verification of FortiAnalyzer by use of certificate.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable identity verification of FortiAnalyzer by use of certificate.</td></tr><tr><td><i>disable</i></td><td>Disable identity verification of FortiAnalyzer by use of certificate.</td></tr></table>	Option	Description	<i>enable</i>	Enable identity verification of FortiAnalyzer by use of certificate.	<i>disable</i>	Disable identity verification of FortiAnalyzer by use of certificate.					
Option	Description											
<i>enable</i>	Enable identity verification of FortiAnalyzer by use of certificate.											
<i>disable</i>	Disable identity verification of FortiAnalyzer by use of certificate.											
conn-timeout	FortiAnalyzer connection time-out in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 3600	10								
enc-algorithm	Configure the level of SSL protection for secure communication with FortiAnalyzer.	option	-	high								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>high-medium</i></td><td>Encrypt logs using high and medium encryption algorithms.</td></tr><tr><td><i>high</i></td><td>Encrypt logs using high encryption algorithms.</td></tr><tr><td><i>low</i></td><td>Encrypt logs using all encryption algorithms.</td></tr></table>	Option	Description	<i>high-medium</i>	Encrypt logs using high and medium encryption algorithms.	<i>high</i>	Encrypt logs using high encryption algorithms.	<i>low</i>	Encrypt logs using all encryption algorithms.			
Option	Description											
<i>high-medium</i>	Encrypt logs using high and medium encryption algorithms.											
<i>high</i>	Encrypt logs using high encryption algorithms.											
<i>low</i>	Encrypt logs using all encryption algorithms.											
hmac-algorithm	FortiAnalyzer IPsec tunnel HMAC algorithm.	option	-	sha256								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>sha256</i></td><td>Use SHA256 as HMAC algorithm.</td></tr><tr><td><i>sha1</i></td><td>Step down to SHA1 as the HMAC algorithm.</td></tr></table>	Option	Description	<i>sha256</i>	Use SHA256 as HMAC algorithm.	<i>sha1</i>	Step down to SHA1 as the HMAC algorithm.					
Option	Description											
<i>sha256</i>	Use SHA256 as HMAC algorithm.											
<i>sha1</i>	Step down to SHA1 as the HMAC algorithm.											
interface	Specify outgoing interface to reach server.	string	Maximum length: 15									
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto								

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto</i></td><td>Set outgoing interface automatically.</td></tr><tr><td><i>sdwan</i></td><td>Set outgoing interface by SD-WAN or policy routing rules.</td></tr><tr><td><i>specify</i></td><td>Set outgoing interface manually.</td></tr></table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.			
	Option	Description										
	<i>auto</i>	Set outgoing interface automatically.										
	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.										
<i>specify</i>	Set outgoing interface manually.											
ips-archive	Enable/disable IPS packet archive logging.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable IPS packet archive logging.</td></tr><tr><td><i>disable</i></td><td>Disable IPS packet archive logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable IPS packet archive logging.	<i>disable</i>	Disable IPS packet archive logging.					
	Option	Description										
	<i>enable</i>	Enable IPS packet archive logging.										
<i>disable</i>	Disable IPS packet archive logging.											
max-log-rate	FortiAnalyzer maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0								
monitor-failure-retry-period	Time between FortiAnalyzer connection retries in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 86400	5								
monitor-keepalive-period	Time between OFTP keepalives in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 120	5								
preshared-key	Preshared-key used for auto-authorization on FortiAnalyzer.	string	Maximum length: 63									
priority	Set log transmission priority.	option	-	default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>Set FortiAnalyzer log transmission priority to default.</td></tr><tr><td><i>low</i></td><td>Set FortiAnalyzer log transmission priority to low.</td></tr></table>	Option	Description	<i>default</i>	Set FortiAnalyzer log transmission priority to default.	<i>low</i>	Set FortiAnalyzer log transmission priority to low.					
	Option	Description										
	<i>default</i>	Set FortiAnalyzer log transmission priority to default.										
<i>low</i>	Set FortiAnalyzer log transmission priority to low.											
reliable	Enable/disable reliable logging to FortiAnalyzer.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable reliable logging to FortiAnalyzer.</td></tr><tr><td><i>disable</i></td><td>Disable reliable logging to FortiAnalyzer.</td></tr></table>	Option	Description	<i>enable</i>	Enable reliable logging to FortiAnalyzer.	<i>disable</i>	Disable reliable logging to FortiAnalyzer.					
	Option	Description										
	<i>enable</i>	Enable reliable logging to FortiAnalyzer.										
<i>disable</i>	Disable reliable logging to FortiAnalyzer.											

Parameter	Description	Type	Size	Default												
serial <name>	Serial numbers of the FortiAnalyzer. Serial Number.	string	Maximum length: 79													
server	The remote FortiAnalyzer.	string	Maximum length: 127													
source-ip	Source IPv4 or IPv6 address used to communicate with FortiAnalyzer.	string	Maximum length: 63													
ssl-min-proto-version	Minimum supported protocol version for SSL/TLS connections.	option	-	default												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>default</td><td>Follow system global setting.</td></tr><tr><td>SSLv3</td><td>SSLv3.</td></tr><tr><td>TLSv1</td><td>TLSv1.</td></tr><tr><td>TLSv1-1</td><td>TLSv1.1.</td></tr><tr><td>TLSv1-2</td><td>TLSv1.2.</td></tr></table>	Option	Description	default	Follow system global setting.	SSLv3	SSLv3.	TLSv1	TLSv1.	TLSv1-1	TLSv1.1.	TLSv1-2	TLSv1.2.			
Option	Description															
default	Follow system global setting.															
SSLv3	SSLv3.															
TLSv1	TLSv1.															
TLSv1-1	TLSv1.1.															
TLSv1-2	TLSv1.2.															
status	Enable/disable logging to FortiAnalyzer.	option	-	disable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable logging to FortiAnalyzer.</td></tr><tr><td>disable</td><td>Disable logging to FortiAnalyzer.</td></tr></table>	Option	Description	enable	Enable logging to FortiAnalyzer.	disable	Disable logging to FortiAnalyzer.									
Option	Description															
enable	Enable logging to FortiAnalyzer.															
disable	Disable logging to FortiAnalyzer.															
upload-day	Day of week (month) to upload logs.	user	Not Specified													
upload-interval	Frequency to upload log files to FortiAnalyzer.	option	-	daily												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>daily</td><td>Upload log files to FortiAnalyzer once a day.</td></tr><tr><td>weekly</td><td>Upload log files to FortiAnalyzer once a week.</td></tr><tr><td>monthly</td><td>Upload log files to FortiAnalyzer once a month.</td></tr></table>	Option	Description	daily	Upload log files to FortiAnalyzer once a day.	weekly	Upload log files to FortiAnalyzer once a week.	monthly	Upload log files to FortiAnalyzer once a month.							
Option	Description															
daily	Upload log files to FortiAnalyzer once a day.															
weekly	Upload log files to FortiAnalyzer once a week.															
monthly	Upload log files to FortiAnalyzer once a month.															
upload-option	Enable/disable logging to hard disk and then uploading to FortiAnalyzer.	option	-	5-minute												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>store-and-upload</td><td>Log to hard disk and then upload to FortiAnalyzer.</td></tr></table>	Option	Description	store-and-upload	Log to hard disk and then upload to FortiAnalyzer.											
Option	Description															
store-and-upload	Log to hard disk and then upload to FortiAnalyzer.															

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>realtime</i>	Log directly to FortiAnalyzer in real time.		
	<i>1-minute</i>	Log directly to FortiAnalyzer at least every 1 minute.		
	<i>5-minute</i>	Log directly to FortiAnalyzer at least every 5 minutes.		
upload-time	Time to upload logs (hh:mm).	user	Not Specified	

## config log fortianalyzer3 filter

Filters for FortiAnalyzer.

```
config log fortianalyzer3 filter
  Description: Filters for FortiAnalyzer.
  set anomaly [enable|disable]
  set dlp-archive [enable|disable]
  set forward-traffic [enable|disable]
  config free-style
    Description: Free style filters.
    edit <id>
      set category [traffic|event|...]
      set filter {string}
      set filter-type [include|exclude]
    next
  end
  set gtp [enable|disable]
  set local-traffic [enable|disable]
  set multicast-traffic [enable|disable]
  set severity [emergency|alert|...]
  set sniffer-traffic [enable|disable]
  set voip [enable|disable]
  set ztna-traffic [enable|disable]
end
```

## config log fortianalyzer3 filter

Parameter	Description	Type	Size	Default
anomaly	Enable/disable anomaly logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable anomaly logging.		
	<i>disable</i>	Disable anomaly logging.		
dlp-archive	Enable/disable DLP archive logging.	option	-	enable

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable DLP archive logging.		
	<i>disable</i>	Disable DLP archive logging.		
forward-traffic	Enable/disable forward traffic logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable forward traffic logging.		
	<i>disable</i>	Disable forward traffic logging.		
gtp *	Enable/disable GTP messages logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable GTP messages logging.		
	<i>disable</i>	Disable GTP messages logging.		
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable local in or out traffic logging.		
	<i>disable</i>	Disable local in or out traffic logging.		
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable multicast traffic logging.		
	<i>disable</i>	Disable multicast traffic logging.		
severity	Lowest severity level to log.	option	-	information
	<b>Option</b>	<b>Description</b>		
	<i>emergency</i>	Emergency level.		
	<i>alert</i>	Alert level.		
	<i>critical</i>	Critical level.		
	<i>error</i>	Error level.		
	<i>warning</i>	Warning level.		
	<i>notification</i>	Notification level.		

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>information</i>	Information level.		
	<i>debug</i>	Debug level.		
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable sniffer traffic logging.		
	<i>disable</i>	Disable sniffer traffic logging.		
voip	Enable/disable VoIP logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable VoIP logging.		
	<i>disable</i>	Disable VoIP logging.		
ztna-traffic	Enable/disable ztna traffic logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable ztna traffic logging.		
	<i>disable</i>	Disable ztna traffic logging.		

\* This parameter may not exist in some models.

### config free-style

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
category	Log category.	option	-	traffic
	<b>Option</b>	<b>Description</b>		
	<i>traffic</i>	Traffic log.		
	<i>event</i>	Event log.		
	<i>virus</i>	Antivirus log.		

Parameter	Description	Type	Size	Default																												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>webfilter</i></td><td>Web filter log.</td></tr><tr><td><i>attack</i></td><td>Attack log.</td></tr><tr><td><i>spam</i></td><td>Antispam log.</td></tr><tr><td><i>anomaly</i></td><td>Anomaly log.</td></tr><tr><td><i>voip</i></td><td>VoIP log.</td></tr><tr><td><i>dlp</i></td><td>DLP log.</td></tr><tr><td><i>app-ctrl</i></td><td>Application control log.</td></tr><tr><td><i>waf</i></td><td>Web application firewall log.</td></tr><tr><td><i>dns</i></td><td>DNS detail log.</td></tr><tr><td><i>ssh</i></td><td>SSH log.</td></tr><tr><td><i>ssl</i></td><td>SSL log.</td></tr><tr><td><i>file-filter</i></td><td>File filter log.</td></tr><tr><td><i>icap</i></td><td>ICAP log.</td></tr></table>	Option	Description	<i>webfilter</i>	Web filter log.	<i>attack</i>	Attack log.	<i>spam</i>	Antispam log.	<i>anomaly</i>	Anomaly log.	<i>voip</i>	VoIP log.	<i>dlp</i>	DLP log.	<i>app-ctrl</i>	Application control log.	<i>waf</i>	Web application firewall log.	<i>dns</i>	DNS detail log.	<i>ssh</i>	SSH log.	<i>ssl</i>	SSL log.	<i>file-filter</i>	File filter log.	<i>icap</i>	ICAP log.			
	Option	Description																														
	<i>webfilter</i>	Web filter log.																														
	<i>attack</i>	Attack log.																														
	<i>spam</i>	Antispam log.																														
	<i>anomaly</i>	Anomaly log.																														
	<i>voip</i>	VoIP log.																														
	<i>dlp</i>	DLP log.																														
	<i>app-ctrl</i>	Application control log.																														
	<i>waf</i>	Web application firewall log.																														
	<i>dns</i>	DNS detail log.																														
	<i>ssh</i>	SSH log.																														
	<i>ssl</i>	SSL log.																														
	<i>file-filter</i>	File filter log.																														
<i>icap</i>	ICAP log.																															
filter	Free style filter string.	string	Maximum length: 1023																													
filter-type	Include/exclude logs that match the filter.	option	-	include																												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>include</i></td><td>Include logs that match the filter.</td></tr><tr><td><i>exclude</i></td><td>Exclude logs that match the filter.</td></tr></table>	Option	Description	<i>include</i>	Include logs that match the filter.	<i>exclude</i>	Exclude logs that match the filter.																									
	Option	Description																														
	<i>include</i>	Include logs that match the filter.																														
<i>exclude</i>	Exclude logs that match the filter.																															

### config log fortianalyzer3 override-filter

Override filters for FortiAnalyzer.

```

config log fortianalyzer3 override-filter
    Description: Override filters for FortiAnalyzer.
    set anomaly [enable|disable]
    set dlp-archive [enable|disable]
    set forward-traffic [enable|disable]
    config free-style
        Description: Free style filters.
        edit <id>
            set category [traffic|event|...]
            set filter {string}
            set filter-type [include|exclude]
        next
    end

```

```

set gtp [enable|disable]
set local-traffic [enable|disable]
set multicast-traffic [enable|disable]
set severity [emergency|alert|...]
set sniffer-traffic [enable|disable]
set voip [enable|disable]
set ztna-traffic [enable|disable]
end

```

## config log fortianalyzer3 override-filter

Parameter	Description	Type	Size	Default
anomaly	Enable/disable anomaly logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable anomaly logging.		
	<i>disable</i>	Disable anomaly logging.		
dlp-archive	Enable/disable DLP archive logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable DLP archive logging.		
	<i>disable</i>	Disable DLP archive logging.		
forward-traffic	Enable/disable forward traffic logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable forward traffic logging.		
	<i>disable</i>	Disable forward traffic logging.		
gtp *	Enable/disable GTP messages logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable GTP messages logging.		
	<i>disable</i>	Disable GTP messages logging.		
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable local in or out traffic logging.		
	<i>disable</i>	Disable local in or out traffic logging.		
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable



Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable multicast traffic logging.		
	<i>disable</i>	Disable multicast traffic logging.		
severity	Lowest severity level to log.	option	-	information
	<b>Option</b>	<b>Description</b>		
	<i>emergency</i>	Emergency level.		
	<i>alert</i>	Alert level.		
	<i>critical</i>	Critical level.		
	<i>error</i>	Error level.		
	<i>warning</i>	Warning level.		
	<i>notification</i>	Notification level.		
	<i>information</i>	Information level.		
	<i>debug</i>	Debug level.		
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable sniffer traffic logging.		
	<i>disable</i>	Disable sniffer traffic logging.		
voip	Enable/disable VoIP logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable VoIP logging.		
	<i>disable</i>	Disable VoIP logging.		
ztna-traffic	Enable/disable ztna traffic logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable ztna traffic logging.		
	<i>disable</i>	Disable ztna traffic logging.		

\* This parameter may not exist in some models.

## config free-style

Parameter	Description	Type	Size	Default																																		
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0																																		
category	Log category.	option	-	traffic																																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>traffic</td><td>Traffic log.</td></tr><tr><td>event</td><td>Event log.</td></tr><tr><td>virus</td><td>Antivirus log.</td></tr><tr><td>webfilter</td><td>Web filter log.</td></tr><tr><td>attack</td><td>Attack log.</td></tr><tr><td>spam</td><td>Antispam log.</td></tr><tr><td>anomaly</td><td>Anomaly log.</td></tr><tr><td>voip</td><td>VoIP log.</td></tr><tr><td>dlp</td><td>DLP log.</td></tr><tr><td>app-ctrl</td><td>Application control log.</td></tr><tr><td>waf</td><td>Web application firewall log.</td></tr><tr><td>dns</td><td>DNS detail log.</td></tr><tr><td>ssh</td><td>SSH log.</td></tr><tr><td>ssl</td><td>SSL log.</td></tr><tr><td>file-filter</td><td>File filter log.</td></tr><tr><td>icap</td><td>ICAP log.</td></tr></table>	Option	Description	traffic	Traffic log.	event	Event log.	virus	Antivirus log.	webfilter	Web filter log.	attack	Attack log.	spam	Antispam log.	anomaly	Anomaly log.	voip	VoIP log.	dlp	DLP log.	app-ctrl	Application control log.	waf	Web application firewall log.	dns	DNS detail log.	ssh	SSH log.	ssl	SSL log.	file-filter	File filter log.	icap	ICAP log.			
	Option	Description																																				
	traffic	Traffic log.																																				
	event	Event log.																																				
	virus	Antivirus log.																																				
	webfilter	Web filter log.																																				
	attack	Attack log.																																				
	spam	Antispam log.																																				
	anomaly	Anomaly log.																																				
	voip	VoIP log.																																				
	dlp	DLP log.																																				
	app-ctrl	Application control log.																																				
	waf	Web application firewall log.																																				
	dns	DNS detail log.																																				
	ssh	SSH log.																																				
	ssl	SSL log.																																				
	file-filter	File filter log.																																				
icap	ICAP log.																																					
filter	Free style filter string.	string	Maximum length: 1023																																			
filter-type	Include/exclude logs that match the filter.	option	-	include																																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>include</td><td>Include logs that match the filter.</td></tr><tr><td>exclude</td><td>Exclude logs that match the filter.</td></tr></table>	Option	Description	include	Include logs that match the filter.	exclude	Exclude logs that match the filter.																															
	Option	Description																																				
	include	Include logs that match the filter.																																				
exclude	Exclude logs that match the filter.																																					

## config log fortianalyzer3 override-setting

Override FortiAnalyzer settings.

```
config log fortianalyzer3 override-setting
  Description: Override FortiAnalyzer settings.
  set access-config [enable|disable]
  set certificate {string}
  set certificate-verification [enable|disable]
  set conn-timeout {integer}
  set enc-algorithm [high-medium|high|...]
  set hmac-algorithm [sha256|sha1]
  set interface {string}
  set interface-select-method [auto|sdwan|...]
  set ips-archive [enable|disable]
  set max-log-rate {integer}
  set monitor-failure-retry-period {integer}
  set monitor-keepalive-period {integer}
  set preshared-key {string}
  set priority [default|low]
  set reliable [enable|disable]
  set serial <name1>, <name2>, ...
  set server {string}
  set source-ip {string}
  set ssl-min-proto-version [default|SSLv3|...]
  set status [enable|disable]
  set upload-day {user}
  set upload-interval [daily|weekly|...]
  set upload-option [store-and-upload|realtime|...]
  set upload-time {user}
  set use-management-vdom [enable|disable]
end
```

## config log fortianalyzer3 override-setting

Parameter	Description	Type	Size	Default
access-config	Enable/disable FortiAnalyzer access to configuration and data.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable FortiAnalyzer access to configuration and data.		
	<i>disable</i>	Disable FortiAnalyzer access to configuration and data.		
certificate	Certificate used to communicate with FortiAnalyzer.	string	Maximum length: 35	
certificate-verification	Enable/disable identity verification of FortiAnalyzer by use of certificate.	option	-	enable

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable identity verification of FortiAnalyzer by use of certificate.</td></tr><tr><td><i>disable</i></td><td>Disable identity verification of FortiAnalyzer by use of certificate.</td></tr></table>	Option	Description	<i>enable</i>	Enable identity verification of FortiAnalyzer by use of certificate.	<i>disable</i>	Disable identity verification of FortiAnalyzer by use of certificate.					
	Option	Description										
	<i>enable</i>	Enable identity verification of FortiAnalyzer by use of certificate.										
<i>disable</i>	Disable identity verification of FortiAnalyzer by use of certificate.											
conn-timeout	FortiAnalyzer connection time-out in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 3600	10								
enc-algorithm	Configure the level of SSL protection for secure communication with FortiAnalyzer.	option	-	high								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>high-medium</i></td><td>Encrypt logs using high and medium encryption algorithms.</td></tr><tr><td><i>high</i></td><td>Encrypt logs using high encryption algorithms.</td></tr><tr><td><i>low</i></td><td>Encrypt logs using all encryption algorithms.</td></tr></table>	Option	Description	<i>high-medium</i>	Encrypt logs using high and medium encryption algorithms.	<i>high</i>	Encrypt logs using high encryption algorithms.	<i>low</i>	Encrypt logs using all encryption algorithms.			
	Option	Description										
	<i>high-medium</i>	Encrypt logs using high and medium encryption algorithms.										
	<i>high</i>	Encrypt logs using high encryption algorithms.										
<i>low</i>	Encrypt logs using all encryption algorithms.											
hmac-algorithm	FortiAnalyzer IPsec tunnel HMAC algorithm.	option	-	sha256								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>sha256</i></td><td>Use SHA256 as HMAC algorithm.</td></tr><tr><td><i>sha1</i></td><td>Step down to SHA1 as the HMAC algorithm.</td></tr></table>	Option	Description	<i>sha256</i>	Use SHA256 as HMAC algorithm.	<i>sha1</i>	Step down to SHA1 as the HMAC algorithm.					
	Option	Description										
	<i>sha256</i>	Use SHA256 as HMAC algorithm.										
<i>sha1</i>	Step down to SHA1 as the HMAC algorithm.											
interface	Specify outgoing interface to reach server.	string	Maximum length: 15									
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto</i></td><td>Set outgoing interface automatically.</td></tr><tr><td><i>sdwan</i></td><td>Set outgoing interface by SD-WAN or policy routing rules.</td></tr><tr><td><i>specify</i></td><td>Set outgoing interface manually.</td></tr></table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.			
	Option	Description										
	<i>auto</i>	Set outgoing interface automatically.										
	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.										
<i>specify</i>	Set outgoing interface manually.											
ips-archive	Enable/disable IPS packet archive logging.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable IPS packet archive logging.</td></tr><tr><td><i>disable</i></td><td>Disable IPS packet archive logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable IPS packet archive logging.	<i>disable</i>	Disable IPS packet archive logging.					
	Option	Description										
	<i>enable</i>	Enable IPS packet archive logging.										
<i>disable</i>	Disable IPS packet archive logging.											

Parameter	Description	Type	Size	Default						
max-log-rate	FortiAnalyzer maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0						
monitor-failure-retry-period	Time between FortiAnalyzer connection retries in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 86400	5						
monitor-keepalive-period	Time between OFTP keepalives in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 120	5						
preshared-key	Preshared-key used for auto-authorization on FortiAnalyzer.	string	Maximum length: 63							
priority	Set log transmission priority.	option	-	default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>default</td><td>Set FortiAnalyzer log transmission priority to default.</td></tr><tr><td>low</td><td>Set FortiAnalyzer log transmission priority to low.</td></tr></table>				Option	Description	default	Set FortiAnalyzer log transmission priority to default.	low	Set FortiAnalyzer log transmission priority to low.
Option	Description									
default	Set FortiAnalyzer log transmission priority to default.									
low	Set FortiAnalyzer log transmission priority to low.									
reliable	Enable/disable reliable logging to FortiAnalyzer.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable reliable logging to FortiAnalyzer.</td></tr><tr><td>disable</td><td>Disable reliable logging to FortiAnalyzer.</td></tr></table>				Option	Description	enable	Enable reliable logging to FortiAnalyzer.	disable	Disable reliable logging to FortiAnalyzer.
Option	Description									
enable	Enable reliable logging to FortiAnalyzer.									
disable	Disable reliable logging to FortiAnalyzer.									
serial <name>	Serial numbers of the FortiAnalyzer. Serial Number.	string	Maximum length: 79							
server	The remote FortiAnalyzer.	string	Maximum length: 127							
source-ip	Source IPv4 or IPv6 address used to communicate with FortiAnalyzer.	string	Maximum length: 63							
ssl-min-protocol-version	Minimum supported protocol version for SSL/TLS connections.	option	-	default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>default</td><td>Follow system global setting.</td></tr></table>				Option	Description	default	Follow system global setting.		
Option	Description									
default	Follow system global setting.									

Parameter	Description	Type	Size	Default										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>SSLv3</td><td>SSLv3.</td></tr><tr><td>TLSv1</td><td>TLSv1.</td></tr><tr><td>TLSv1-1</td><td>TLSv1.1.</td></tr><tr><td>TLSv1-2</td><td>TLSv1.2.</td></tr></table>	Option	Description	SSLv3	SSLv3.	TLSv1	TLSv1.	TLSv1-1	TLSv1.1.	TLSv1-2	TLSv1.2.			
	Option	Description												
	SSLv3	SSLv3.												
	TLSv1	TLSv1.												
	TLSv1-1	TLSv1.1.												
TLSv1-2	TLSv1.2.													
status	Enable/disable logging to FortiAnalyzer.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable logging to FortiAnalyzer.</td></tr><tr><td>disable</td><td>Disable logging to FortiAnalyzer.</td></tr></table>	Option	Description	enable	Enable logging to FortiAnalyzer.	disable	Disable logging to FortiAnalyzer.							
	Option	Description												
	enable	Enable logging to FortiAnalyzer.												
disable	Disable logging to FortiAnalyzer.													
upload-day	Day of week (month) to upload logs.	user	Not Specified											
upload-interval	Frequency to upload log files to FortiAnalyzer.	option	-	daily										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>daily</td><td>Upload log files to FortiAnalyzer once a day.</td></tr><tr><td>weekly</td><td>Upload log files to FortiAnalyzer once a week.</td></tr><tr><td>monthly</td><td>Upload log files to FortiAnalyzer once a month.</td></tr></table>	Option	Description	daily	Upload log files to FortiAnalyzer once a day.	weekly	Upload log files to FortiAnalyzer once a week.	monthly	Upload log files to FortiAnalyzer once a month.					
	Option	Description												
	daily	Upload log files to FortiAnalyzer once a day.												
	weekly	Upload log files to FortiAnalyzer once a week.												
monthly	Upload log files to FortiAnalyzer once a month.													
upload-option	Enable/disable logging to hard disk and then uploading to FortiAnalyzer.	option	-	5-minute										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>store-and-upload</td><td>Log to hard disk and then upload to FortiAnalyzer.</td></tr><tr><td>realtime</td><td>Log directly to FortiAnalyzer in real time.</td></tr><tr><td>1-minute</td><td>Log directly to FortiAnalyzer at least every 1 minute.</td></tr><tr><td>5-minute</td><td>Log directly to FortiAnalyzer at least every 5 minutes.</td></tr></table>	Option	Description	store-and-upload	Log to hard disk and then upload to FortiAnalyzer.	realtime	Log directly to FortiAnalyzer in real time.	1-minute	Log directly to FortiAnalyzer at least every 1 minute.	5-minute	Log directly to FortiAnalyzer at least every 5 minutes.			
	Option	Description												
	store-and-upload	Log to hard disk and then upload to FortiAnalyzer.												
	realtime	Log directly to FortiAnalyzer in real time.												
	1-minute	Log directly to FortiAnalyzer at least every 1 minute.												
5-minute	Log directly to FortiAnalyzer at least every 5 minutes.													
upload-time	Time to upload logs (hh:mm).	user	Not Specified											
use-management-vdom	Enable/disable use of management VDOM IP address as source IP for logs sent to FortiAnalyzer.	option	-	disable										

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Enable use of management VDOM IP address as source IP for logs sent to FortiAnalyzer.		
	<i>disable</i>	Disable use of management VDOM IP address as source IP for logs sent to FortiAnalyzer.		

## config log fortianalyzer3 setting

Global FortiAnalyzer settings.

```
config log fortianalyzer3 setting
    Description: Global FortiAnalyzer settings.
    set access-config [enable|disable]
    set certificate {string}
    set certificate-verification [enable|disable]
    set conn-timeout {integer}
    set enc-algorithm [high-medium|high|...]
    set hmac-algorithm [sha256|sha1]
    set interface {string}
    set interface-select-method [auto|sdwan|...]
    set ips-archive [enable|disable]
    set max-log-rate {integer}
    set monitor-failure-retry-period {integer}
    set monitor-keepalive-period {integer}
    set preshared-key {string}
    set priority [default|low]
    set reliable [enable|disable]
    set serial <name1>, <name2>, ...
    set server {string}
    set source-ip {string}
    set ssl-min-proto-version [default|SSLv3|...]
    set status [enable|disable]
    set upload-day {user}
    set upload-interval [daily|weekly|...]
    set upload-option [store-and-upload|realtime|...]
    set upload-time {user}
end
```

## config log fortianalyzer3 setting

Parameter	Description	Type	Size	Default
access-config	Enable/disable FortiAnalyzer access to configuration and data.	option	-	enable

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable FortiAnalyzer access to configuration and data.		
	<i>disable</i>	Disable FortiAnalyzer access to configuration and data.		
certificate	Certificate used to communicate with FortiAnalyzer.	string	Maximum length: 35	
certificate-verification	Enable/disable identity verification of FortiAnalyzer by use of certificate.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable identity verification of FortiAnalyzer by use of certificate.		
	<i>disable</i>	Disable identity verification of FortiAnalyzer by use of certificate.		
conn-timeout	FortiAnalyzer connection time-out in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 3600	10
enc-algorithm	Configure the level of SSL protection for secure communication with FortiAnalyzer.	option	-	high
	<b>Option</b>	<b>Description</b>		
	<i>high-medium</i>	Encrypt logs using high and medium encryption algorithms.		
	<i>high</i>	Encrypt logs using high encryption algorithms.		
	<i>low</i>	Encrypt logs using all encryption algorithms.		
hmac-algorithm	FortiAnalyzer IPsec tunnel HMAC algorithm.	option	-	sha256
	<b>Option</b>	<b>Description</b>		
	<i>sha256</i>	Use SHA256 as HMAC algorithm.		
	<i>sha1</i>	Step down to SHA1 as the HMAC algorithm.		
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto
	<b>Option</b>	<b>Description</b>		
	<i>auto</i>	Set outgoing interface automatically.		



Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.		
	<i>specify</i>	Set outgoing interface manually.		
ips-archive	Enable/disable IPS packet archive logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable IPS packet archive logging.		
	<i>disable</i>	Disable IPS packet archive logging.		
max-log-rate	FortiAnalyzer maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0
monitor-failure-retry-period	Time between FortiAnalyzer connection retries in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 86400	5
monitor-keepalive-period	Time between OFTP keepalives in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 120	5
preshared-key	Preshared-key used for auto-authorization on FortiAnalyzer.	string	Maximum length: 63	
priority	Set log transmission priority.	option	-	default
	<b>Option</b>	<b>Description</b>		
	<i>default</i>	Set FortiAnalyzer log transmission priority to default.		
	<i>low</i>	Set FortiAnalyzer log transmission priority to low.		
reliable	Enable/disable reliable logging to FortiAnalyzer.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable reliable logging to FortiAnalyzer.		
	<i>disable</i>	Disable reliable logging to FortiAnalyzer.		
serial <name>	Serial numbers of the FortiAnalyzer. Serial Number.	string	Maximum length: 79	

Parameter	Description	Type	Size	Default												
server	The remote FortiAnalyzer.	string	Maximum length: 127													
source-ip	Source IPv4 or IPv6 address used to communicate with FortiAnalyzer.	string	Maximum length: 63													
ssl-min-protocol-version	Minimum supported protocol version for SSL/TLS connections.	option	-	default												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>default</td><td>Follow system global setting.</td></tr><tr><td>SSLv3</td><td>SSLv3.</td></tr><tr><td>TLSv1</td><td>TLSv1.</td></tr><tr><td>TLSv1-1</td><td>TLSv1.1.</td></tr><tr><td>TLSv1-2</td><td>TLSv1.2.</td></tr></table>	Option	Description	default	Follow system global setting.	SSLv3	SSLv3.	TLSv1	TLSv1.	TLSv1-1	TLSv1.1.	TLSv1-2	TLSv1.2.			
Option	Description															
default	Follow system global setting.															
SSLv3	SSLv3.															
TLSv1	TLSv1.															
TLSv1-1	TLSv1.1.															
TLSv1-2	TLSv1.2.															
status	Enable/disable logging to FortiAnalyzer.	option	-	disable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable logging to FortiAnalyzer.</td></tr><tr><td>disable</td><td>Disable logging to FortiAnalyzer.</td></tr></table>	Option	Description	enable	Enable logging to FortiAnalyzer.	disable	Disable logging to FortiAnalyzer.									
Option	Description															
enable	Enable logging to FortiAnalyzer.															
disable	Disable logging to FortiAnalyzer.															
upload-day	Day of week (month) to upload logs.	user	Not Specified													
upload-interval	Frequency to upload log files to FortiAnalyzer.	option	-	daily												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>daily</td><td>Upload log files to FortiAnalyzer once a day.</td></tr><tr><td>weekly</td><td>Upload log files to FortiAnalyzer once a week.</td></tr><tr><td>monthly</td><td>Upload log files to FortiAnalyzer once a month.</td></tr></table>	Option	Description	daily	Upload log files to FortiAnalyzer once a day.	weekly	Upload log files to FortiAnalyzer once a week.	monthly	Upload log files to FortiAnalyzer once a month.							
Option	Description															
daily	Upload log files to FortiAnalyzer once a day.															
weekly	Upload log files to FortiAnalyzer once a week.															
monthly	Upload log files to FortiAnalyzer once a month.															
upload-option	Enable/disable logging to hard disk and then uploading to FortiAnalyzer.	option	-	5-minute												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>store-and-upload</td><td>Log to hard disk and then upload to FortiAnalyzer.</td></tr><tr><td>realtime</td><td>Log directly to FortiAnalyzer in real time.</td></tr><tr><td>1-minute</td><td>Log directly to FortiAnalyzer at least every 1 minute.</td></tr><tr><td>5-minute</td><td>Log directly to FortiAnalyzer at least every 5 minutes.</td></tr></table>	Option	Description	store-and-upload	Log to hard disk and then upload to FortiAnalyzer.	realtime	Log directly to FortiAnalyzer in real time.	1-minute	Log directly to FortiAnalyzer at least every 1 minute.	5-minute	Log directly to FortiAnalyzer at least every 5 minutes.					
Option	Description															
store-and-upload	Log to hard disk and then upload to FortiAnalyzer.															
realtime	Log directly to FortiAnalyzer in real time.															
1-minute	Log directly to FortiAnalyzer at least every 1 minute.															
5-minute	Log directly to FortiAnalyzer at least every 5 minutes.															

Parameter	Description	Type	Size	Default
upload-time	Time to upload logs (hh:mm).	user	Not Specified	

## config log fortianalyzer filter

Filters for FortiAnalyzer.

```
config log fortianalyzer filter
    Description: Filters for FortiAnalyzer.
    set anomaly [enable|disable]
    set dlp-archive [enable|disable]
    set forward-traffic [enable|disable]
    config free-style
        Description: Free style filters.
        edit <id>
            set category [traffic|event|...]
            set filter {string}
            set filter-type [include|exclude]
        next
    end
    set gtp [enable|disable]
    set local-traffic [enable|disable]
    set multicast-traffic [enable|disable]
    set severity [emergency|alert|...]
    set sniffer-traffic [enable|disable]
    set voip [enable|disable]
    set ztna-traffic [enable|disable]
end
```

## config log fortianalyzer filter

Parameter	Description	Type	Size	Default
anomaly	Enable/disable anomaly logging.	option	-	enable
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Enable anomaly logging.		
	<i>disable</i>	Disable anomaly logging.		
dlp-archive	Enable/disable DLP archive logging.	option	-	enable
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Enable DLP archive logging.		
	<i>disable</i>	Disable DLP archive logging.		
forward-traffic	Enable/disable forward traffic logging.	option	-	enable

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable forward traffic logging.		
	<i>disable</i>	Disable forward traffic logging.		
gtp *	Enable/disable GTP messages logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable GTP messages logging.		
	<i>disable</i>	Disable GTP messages logging.		
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable local in or out traffic logging.		
	<i>disable</i>	Disable local in or out traffic logging.		
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable multicast traffic logging.		
	<i>disable</i>	Disable multicast traffic logging.		
severity	Lowest severity level to log.	option	-	information
	<b>Option</b>	<b>Description</b>		
	<i>emergency</i>	Emergency level.		
	<i>alert</i>	Alert level.		
	<i>critical</i>	Critical level.		
	<i>error</i>	Error level.		
	<i>warning</i>	Warning level.		
	<i>notification</i>	Notification level.		
	<i>information</i>	Information level.		
	<i>debug</i>	Debug level.		
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable sniffer traffic logging.		
	<i>disable</i>	Disable sniffer traffic logging.		
voip	Enable/disable VoIP logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable VoIP logging.		
	<i>disable</i>	Disable VoIP logging.		
ztna-traffic	Enable/disable ztna traffic logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable ztna traffic logging.		
	<i>disable</i>	Disable ztna traffic logging.		

\* This parameter may not exist in some models.

### config free-style

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
category	Log category.	option	-	traffic
	<b>Option</b>	<b>Description</b>		
	<i>traffic</i>	Traffic log.		
	<i>event</i>	Event log.		
	<i>virus</i>	Antivirus log.		
	<i>webfilter</i>	Web filter log.		
	<i>attack</i>	Attack log.		
	<i>spam</i>	Antispam log.		
	<i>anomaly</i>	Anomaly log.		
	<i>voip</i>	VoIP log.		

Parameter	Description	Type	Size	Default																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>dlp</i></td><td>DLP log.</td></tr><tr><td><i>app-ctrl</i></td><td>Application control log.</td></tr><tr><td><i>waf</i></td><td>Web application firewall log.</td></tr><tr><td><i>dns</i></td><td>DNS detail log.</td></tr><tr><td><i>ssh</i></td><td>SSH log.</td></tr><tr><td><i>ssl</i></td><td>SSL log.</td></tr><tr><td><i>file-filter</i></td><td>File filter log.</td></tr><tr><td><i>icap</i></td><td>ICAP log.</td></tr></table>	Option	Description	<i>dlp</i>	DLP log.	<i>app-ctrl</i>	Application control log.	<i>waf</i>	Web application firewall log.	<i>dns</i>	DNS detail log.	<i>ssh</i>	SSH log.	<i>ssl</i>	SSL log.	<i>file-filter</i>	File filter log.	<i>icap</i>	ICAP log.			
	Option	Description																				
	<i>dlp</i>	DLP log.																				
	<i>app-ctrl</i>	Application control log.																				
	<i>waf</i>	Web application firewall log.																				
	<i>dns</i>	DNS detail log.																				
	<i>ssh</i>	SSH log.																				
	<i>ssl</i>	SSL log.																				
	<i>file-filter</i>	File filter log.																				
<i>icap</i>	ICAP log.																					
filter	Free style filter string.	string	Maximum length: 1023																			
filter-type	Include/exclude logs that match the filter.	option	-	include																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>include</i></td><td>Include logs that match the filter.</td></tr><tr><td><i>exclude</i></td><td>Exclude logs that match the filter.</td></tr></table>	Option	Description	<i>include</i>	Include logs that match the filter.	<i>exclude</i>	Exclude logs that match the filter.															
	Option	Description																				
	<i>include</i>	Include logs that match the filter.																				
<i>exclude</i>	Exclude logs that match the filter.																					

## config log fortianalyzer override-filter

Override filters for FortiAnalyzer.

```

config log fortianalyzer override-filter
    Description: Override filters for FortiAnalyzer.
    set anomaly [enable|disable]
    set dlp-archive [enable|disable]
    set forward-traffic [enable|disable]
    config free-style
        Description: Free style filters.
        edit <id>
            set category [traffic|event|...]
            set filter {string}
            set filter-type [include|exclude]
        next
    end
    set gtp [enable|disable]
    set local-traffic [enable|disable]
    set multicast-traffic [enable|disable]
    set severity [emergency|alert|...]
    set sniffer-traffic [enable|disable]
    set voip [enable|disable]
    set ztna-traffic [enable|disable]
end

```

## config log fortianalyzer override-filter

Parameter	Description	Type	Size	Default						
anomaly	Enable/disable anomaly logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable anomaly logging.</td></tr><tr><td><i>disable</i></td><td>Disable anomaly logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable anomaly logging.	<i>disable</i>	Disable anomaly logging.			
Option	Description									
<i>enable</i>	Enable anomaly logging.									
<i>disable</i>	Disable anomaly logging.									
dlp-archive	Enable/disable DLP archive logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable DLP archive logging.</td></tr><tr><td><i>disable</i></td><td>Disable DLP archive logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable DLP archive logging.	<i>disable</i>	Disable DLP archive logging.			
Option	Description									
<i>enable</i>	Enable DLP archive logging.									
<i>disable</i>	Disable DLP archive logging.									
forward-traffic	Enable/disable forward traffic logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable forward traffic logging.</td></tr><tr><td><i>disable</i></td><td>Disable forward traffic logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable forward traffic logging.	<i>disable</i>	Disable forward traffic logging.			
Option	Description									
<i>enable</i>	Enable forward traffic logging.									
<i>disable</i>	Disable forward traffic logging.									
gtp *	Enable/disable GTP messages logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable GTP messages logging.</td></tr><tr><td><i>disable</i></td><td>Disable GTP messages logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable GTP messages logging.	<i>disable</i>	Disable GTP messages logging.			
Option	Description									
<i>enable</i>	Enable GTP messages logging.									
<i>disable</i>	Disable GTP messages logging.									
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable local in or out traffic logging.</td></tr><tr><td><i>disable</i></td><td>Disable local in or out traffic logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable local in or out traffic logging.	<i>disable</i>	Disable local in or out traffic logging.			
Option	Description									
<i>enable</i>	Enable local in or out traffic logging.									
<i>disable</i>	Disable local in or out traffic logging.									
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable multicast traffic logging.</td></tr><tr><td><i>disable</i></td><td>Disable multicast traffic logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable multicast traffic logging.	<i>disable</i>	Disable multicast traffic logging.			
Option	Description									
<i>enable</i>	Enable multicast traffic logging.									
<i>disable</i>	Disable multicast traffic logging.									
severity	Lowest severity level to log.	option	-	information						

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>emergency</i>	Emergency level.		
	<i>alert</i>	Alert level.		
	<i>critical</i>	Critical level.		
	<i>error</i>	Error level.		
	<i>warning</i>	Warning level.		
	<i>notification</i>	Notification level.		
	<i>information</i>	Information level.		
	<i>debug</i>	Debug level.		
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable sniffer traffic logging.		
	<i>disable</i>	Disable sniffer traffic logging.		
voip	Enable/disable VoIP logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable VoIP logging.		
	<i>disable</i>	Disable VoIP logging.		
ztna-traffic	Enable/disable ztna traffic logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable ztna traffic logging.		
	<i>disable</i>	Disable ztna traffic logging.		

\* This parameter may not exist in some models.

### config free-style

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0



Parameter	Description	Type	Size	Default																																			
category	Log category.	option	-	traffic																																			
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>traffic</td><td>Traffic log.</td></tr><tr><td>event</td><td>Event log.</td></tr><tr><td>virus</td><td>Antivirus log.</td></tr><tr><td>webfilter</td><td>Web filter log.</td></tr><tr><td>attack</td><td>Attack log.</td></tr><tr><td>spam</td><td>Antispam log.</td></tr><tr><td>anomaly</td><td>Anomaly log.</td></tr><tr><td>voip</td><td>VoIP log.</td></tr><tr><td>dlp</td><td>DLP log.</td></tr><tr><td>app-ctrl</td><td>Application control log.</td></tr><tr><td>waf</td><td>Web application firewall log.</td></tr><tr><td>dns</td><td>DNS detail log.</td></tr><tr><td>ssh</td><td>SSH log.</td></tr><tr><td>ssl</td><td>SSL log.</td></tr><tr><td>file-filter</td><td>File filter log.</td></tr><tr><td>icap</td><td>ICAP log.</td></tr></table>	Option	Description	traffic	Traffic log.	event	Event log.	virus	Antivirus log.	webfilter	Web filter log.	attack	Attack log.	spam	Antispam log.	anomaly	Anomaly log.	voip	VoIP log.	dlp	DLP log.	app-ctrl	Application control log.	waf	Web application firewall log.	dns	DNS detail log.	ssh	SSH log.	ssl	SSL log.	file-filter	File filter log.	icap	ICAP log.				
	Option	Description																																					
	traffic	Traffic log.																																					
	event	Event log.																																					
	virus	Antivirus log.																																					
	webfilter	Web filter log.																																					
	attack	Attack log.																																					
	spam	Antispam log.																																					
	anomaly	Anomaly log.																																					
	voip	VoIP log.																																					
	dlp	DLP log.																																					
	app-ctrl	Application control log.																																					
	waf	Web application firewall log.																																					
	dns	DNS detail log.																																					
	ssh	SSH log.																																					
	ssl	SSL log.																																					
	file-filter	File filter log.																																					
icap	ICAP log.																																						
filter	Free style filter string.	string	Maximum length: 1023																																				
filter-type	Include/exclude logs that match the filter.	option	-	include																																			
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>include</td><td>Include logs that match the filter.</td></tr><tr><td>exclude</td><td>Exclude logs that match the filter.</td></tr></table>	Option	Description	include	Include logs that match the filter.	exclude	Exclude logs that match the filter.																																
	Option	Description																																					
	include	Include logs that match the filter.																																					
exclude	Exclude logs that match the filter.																																						

## config log fortianalyzer override-setting

Override FortiAnalyzer settings.

```
config log fortianalyzer override-setting
    Description: Override FortiAnalyzer settings.
    set access-config [enable|disable]
    set certificate {string}
    set certificate-verification [enable|disable]
    set conn-timeout {integer}
```

```

set enc-algorithm [high-medium|high|...]
set hmac-algorithm [sha256|sha1]
set interface {string}
set interface-select-method [auto|sdwan|...]
set ips-archive [enable|disable]
set max-log-rate {integer}
set monitor-failure-retry-period {integer}
set monitor-keepalive-period {integer}
set preshared-key {string}
set priority [default|low]
set reliable [enable|disable]
set serial <name1>, <name2>, ...
set server {string}
set source-ip {string}
set ssl-min-proto-version [default|SSLv3|...]
set status [enable|disable]
set upload-day {user}
set upload-interval [daily|weekly|...]
set upload-option [store-and-upload|realtime|...]
set upload-time {user}
set use-management-vdom [enable|disable]

```

end

## config log fortianalyzer override-setting

Parameter	Description	Type	Size	Default						
access-config	Enable/disable FortiAnalyzer access to configuration and data.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable FortiAnalyzer access to configuration and data.</td></tr><tr><td>disable</td><td>Disable FortiAnalyzer access to configuration and data.</td></tr></table>	Option	Description	enable	Enable FortiAnalyzer access to configuration and data.	disable	Disable FortiAnalyzer access to configuration and data.			
Option	Description									
enable	Enable FortiAnalyzer access to configuration and data.									
disable	Disable FortiAnalyzer access to configuration and data.									
certificate	Certificate used to communicate with FortiAnalyzer.	string	Maximum length: 35							
certificate-verification	Enable/disable identity verification of FortiAnalyzer by use of certificate.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable identity verification of FortiAnalyzer by use of certificate.</td></tr><tr><td>disable</td><td>Disable identity verification of FortiAnalyzer by use of certificate.</td></tr></table>	Option	Description	enable	Enable identity verification of FortiAnalyzer by use of certificate.	disable	Disable identity verification of FortiAnalyzer by use of certificate.			
Option	Description									
enable	Enable identity verification of FortiAnalyzer by use of certificate.									
disable	Disable identity verification of FortiAnalyzer by use of certificate.									
conn-timeout	FortiAnalyzer connection time-out in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 3600	10						

Parameter	Description	Type	Size	Default								
enc-algorithm	Configure the level of SSL protection for secure communication with FortiAnalyzer.	option	-	high								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>high-medium</td><td>Encrypt logs using high and medium encryption algorithms.</td></tr><tr><td>high</td><td>Encrypt logs using high encryption algorithms.</td></tr><tr><td>low</td><td>Encrypt logs using all encryption algorithms.</td></tr></table>	Option	Description	high-medium	Encrypt logs using high and medium encryption algorithms.	high	Encrypt logs using high encryption algorithms.	low	Encrypt logs using all encryption algorithms.			
Option	Description											
high-medium	Encrypt logs using high and medium encryption algorithms.											
high	Encrypt logs using high encryption algorithms.											
low	Encrypt logs using all encryption algorithms.											
hmac-algorithm	FortiAnalyzer IPsec tunnel HMAC algorithm.	option	-	sha256								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>sha256</td><td>Use SHA256 as HMAC algorithm.</td></tr><tr><td>sha1</td><td>Step down to SHA1 as the HMAC algorithm.</td></tr></table>	Option	Description	sha256	Use SHA256 as HMAC algorithm.	sha1	Step down to SHA1 as the HMAC algorithm.					
Option	Description											
sha256	Use SHA256 as HMAC algorithm.											
sha1	Step down to SHA1 as the HMAC algorithm.											
interface	Specify outgoing interface to reach server.	string	Maximum length: 15									
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>auto</td><td>Set outgoing interface automatically.</td></tr><tr><td>sdwan</td><td>Set outgoing interface by SD-WAN or policy routing rules.</td></tr><tr><td>specify</td><td>Set outgoing interface manually.</td></tr></table>	Option	Description	auto	Set outgoing interface automatically.	sdwan	Set outgoing interface by SD-WAN or policy routing rules.	specify	Set outgoing interface manually.			
Option	Description											
auto	Set outgoing interface automatically.											
sdwan	Set outgoing interface by SD-WAN or policy routing rules.											
specify	Set outgoing interface manually.											
ips-archive	Enable/disable IPS packet archive logging.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable IPS packet archive logging.</td></tr><tr><td>disable</td><td>Disable IPS packet archive logging.</td></tr></table>	Option	Description	enable	Enable IPS packet archive logging.	disable	Disable IPS packet archive logging.					
Option	Description											
enable	Enable IPS packet archive logging.											
disable	Disable IPS packet archive logging.											
max-log-rate	FortiAnalyzer maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0								
monitor-failure-retry-period	Time between FortiAnalyzer connection retries in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 86400	5								

Parameter	Description	Type	Size	Default
monitor-keepalive-period	Time between OFTP keepalives in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 120	5
preshared-key	Preshared-key used for auto-authorization on FortiAnalyzer.	string	Maximum length: 63	
priority	Set log transmission priority.	option	-	default
	<b>Option</b> <b>Description</b>			
	default	Set FortiAnalyzer log transmission priority to default.		
	low	Set FortiAnalyzer log transmission priority to low.		
reliable	Enable/disable reliable logging to FortiAnalyzer.	option	-	disable
	<b>Option</b> <b>Description</b>			
	enable	Enable reliable logging to FortiAnalyzer.		
	disable	Disable reliable logging to FortiAnalyzer.		
serial <name>	Serial numbers of the FortiAnalyzer. Serial Number.	string	Maximum length: 79	
server	The remote FortiAnalyzer.	string	Maximum length: 127	
source-ip	Source IPv4 or IPv6 address used to communicate with FortiAnalyzer.	string	Maximum length: 63	
ssl-min-protocol-version	Minimum supported protocol version for SSL/TLS connections.	option	-	default
	<b>Option</b> <b>Description</b>			
	default	Follow system global setting.		
	SSLv3	SSLv3.		
	TLSv1	TLSv1.		
	TLSv1-1	TLSv1.1.		
	TLSv1-2	TLSv1.2.		
status	Enable/disable logging to FortiAnalyzer.	option	-	disable
	<b>Option</b> <b>Description</b>			
	enable	Enable logging to FortiAnalyzer.		
	disable	Disable logging to FortiAnalyzer.		

Parameter	Description	Type	Size	Default										
upload-day	Day of week (month) to upload logs.	user	Not Specified											
upload-interval	Frequency to upload log files to FortiAnalyzer.	option	-	daily										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>daily</td><td>Upload log files to FortiAnalyzer once a day.</td></tr><tr><td>weekly</td><td>Upload log files to FortiAnalyzer once a week.</td></tr><tr><td>monthly</td><td>Upload log files to FortiAnalyzer once a month.</td></tr></table>	Option	Description	daily	Upload log files to FortiAnalyzer once a day.	weekly	Upload log files to FortiAnalyzer once a week.	monthly	Upload log files to FortiAnalyzer once a month.					
Option	Description													
daily	Upload log files to FortiAnalyzer once a day.													
weekly	Upload log files to FortiAnalyzer once a week.													
monthly	Upload log files to FortiAnalyzer once a month.													
upload-option	Enable/disable logging to hard disk and then uploading to FortiAnalyzer.	option	-	5-minute										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>store-and-upload</td><td>Log to hard disk and then upload to FortiAnalyzer.</td></tr><tr><td>realtime</td><td>Log directly to FortiAnalyzer in real time.</td></tr><tr><td>1-minute</td><td>Log directly to FortiAnalyzer at least every 1 minute.</td></tr><tr><td>5-minute</td><td>Log directly to FortiAnalyzer at least every 5 minutes.</td></tr></table>	Option	Description	store-and-upload	Log to hard disk and then upload to FortiAnalyzer.	realtime	Log directly to FortiAnalyzer in real time.	1-minute	Log directly to FortiAnalyzer at least every 1 minute.	5-minute	Log directly to FortiAnalyzer at least every 5 minutes.			
Option	Description													
store-and-upload	Log to hard disk and then upload to FortiAnalyzer.													
realtime	Log directly to FortiAnalyzer in real time.													
1-minute	Log directly to FortiAnalyzer at least every 1 minute.													
5-minute	Log directly to FortiAnalyzer at least every 5 minutes.													
upload-time	Time to upload logs (hh:mm).	user	Not Specified											
use-management-vdom	Enable/disable use of management VDOM IP address as source IP for logs sent to FortiAnalyzer.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable use of management VDOM IP address as source IP for logs sent to FortiAnalyzer.</td></tr><tr><td>disable</td><td>Disable use of management VDOM IP address as source IP for logs sent to FortiAnalyzer.</td></tr></table>	Option	Description	enable	Enable use of management VDOM IP address as source IP for logs sent to FortiAnalyzer.	disable	Disable use of management VDOM IP address as source IP for logs sent to FortiAnalyzer.							
Option	Description													
enable	Enable use of management VDOM IP address as source IP for logs sent to FortiAnalyzer.													
disable	Disable use of management VDOM IP address as source IP for logs sent to FortiAnalyzer.													

## config log fortianalyzer setting

Global FortiAnalyzer settings.

```
config log fortianalyzer setting
  Description: Global FortiAnalyzer settings.
  set access-config [enable|disable]
  set certificate {string}
  set certificate-verification [enable|disable]
  set conn-timeout {integer}
  set enc-algorithm [high-medium|high|...]
```

```

set hmac-algorithm [sha256|sha1]
set interface {string}
set interface-select-method [auto|sdwan|...]
set ips-archive [enable|disable]
set max-log-rate {integer}
set monitor-failure-retry-period {integer}
set monitor-keepalive-period {integer}
set preshared-key {string}
set priority [default|low]
set reliable [enable|disable]
set serial <name1>, <name2>, ...
set server {string}
set source-ip {string}
set ssl-min-proto-version [default|SSLv3|...]
set status [enable|disable]
set upload-day {user}
set upload-interval [daily|weekly|...]
set upload-option [store-and-upload|realtime|...]
set upload-time {user}

```

end

## config log fortianalyzer setting

Parameter	Description	Type	Size	Default						
access-config	Enable/disable FortiAnalyzer access to configuration and data.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable FortiAnalyzer access to configuration and data.</td></tr><tr><td><i>disable</i></td><td>Disable FortiAnalyzer access to configuration and data.</td></tr></table>	Option	Description	<i>enable</i>	Enable FortiAnalyzer access to configuration and data.	<i>disable</i>	Disable FortiAnalyzer access to configuration and data.			
Option	Description									
<i>enable</i>	Enable FortiAnalyzer access to configuration and data.									
<i>disable</i>	Disable FortiAnalyzer access to configuration and data.									
certificate	Certificate used to communicate with FortiAnalyzer.	string	Maximum length: 35							
certificate-verification	Enable/disable identity verification of FortiAnalyzer by use of certificate.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable identity verification of FortiAnalyzer by use of certificate.</td></tr><tr><td><i>disable</i></td><td>Disable identity verification of FortiAnalyzer by use of certificate.</td></tr></table>	Option	Description	<i>enable</i>	Enable identity verification of FortiAnalyzer by use of certificate.	<i>disable</i>	Disable identity verification of FortiAnalyzer by use of certificate.			
Option	Description									
<i>enable</i>	Enable identity verification of FortiAnalyzer by use of certificate.									
<i>disable</i>	Disable identity verification of FortiAnalyzer by use of certificate.									
conn-timeout	FortiAnalyzer connection time-out in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 3600	10						
enc-algorithm	Configure the level of SSL protection for secure communication with FortiAnalyzer.	option	-	high						

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>high-medium</i>	Encrypt logs using high and medium encryption algorithms.		
	<i>high</i>	Encrypt logs using high encryption algorithms.		
	<i>low</i>	Encrypt logs using all encryption algorithms.		
hmac-algorithm	FortiAnalyzer IPsec tunnel HMAC algorithm.	option	-	sha256
	<b>Option</b>	<b>Description</b>		
	<i>sha256</i>	Use SHA256 as HMAC algorithm.		
	<i>sha1</i>	Step down to SHA1 as the HMAC algorithm.		
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto
	<b>Option</b>	<b>Description</b>		
	<i>auto</i>	Set outgoing interface automatically.		
	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.		
	<i>specify</i>	Set outgoing interface manually.		
ips-archive	Enable/disable IPS packet archive logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable IPS packet archive logging.		
	<i>disable</i>	Disable IPS packet archive logging.		
max-log-rate	FortiAnalyzer maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0
monitor-failure-retry-period	Time between FortiAnalyzer connection retries in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 86400	5

Parameter	Description	Type	Size	Default
monitor-keepalive-period	Time between OFTP keepalives in seconds (for status and log buffer).	integer	Minimum value: 1 Maximum value: 120	5
preshared-key	Preshared-key used for auto-authorization on FortiAnalyzer.	string	Maximum length: 63	
priority	Set log transmission priority.	option	-	default
	<b>Option</b>	<b>Description</b>		
	<i>default</i>	Set FortiAnalyzer log transmission priority to default.		
	<i>low</i>	Set FortiAnalyzer log transmission priority to low.		
reliable	Enable/disable reliable logging to FortiAnalyzer.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable reliable logging to FortiAnalyzer.		
	<i>disable</i>	Disable reliable logging to FortiAnalyzer.		
serial <name>	Serial numbers of the FortiAnalyzer. Serial Number.	string	Maximum length: 79	
server	The remote FortiAnalyzer.	string	Maximum length: 127	
source-ip	Source IPv4 or IPv6 address used to communicate with FortiAnalyzer.	string	Maximum length: 63	
ssl-min-protocol-version	Minimum supported protocol version for SSL/TLS connections.	option	-	default
	<b>Option</b>	<b>Description</b>		
	<i>default</i>	Follow system global setting.		
	<i>SSLv3</i>	SSLv3.		
	<i>TLSv1</i>	TLSv1.		
	<i>TLSv1-1</i>	TLSv1.1.		
	<i>TLSv1-2</i>	TLSv1.2.		
status	Enable/disable logging to FortiAnalyzer.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable logging to FortiAnalyzer.		
	<i>disable</i>	Disable logging to FortiAnalyzer.		



Parameter	Description	Type	Size	Default										
upload-day	Day of week (month) to upload logs.	user	Not Specified											
upload-interval	Frequency to upload log files to FortiAnalyzer.	option	-	daily										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>daily</td><td>Upload log files to FortiAnalyzer once a day.</td></tr><tr><td>weekly</td><td>Upload log files to FortiAnalyzer once a week.</td></tr><tr><td>monthly</td><td>Upload log files to FortiAnalyzer once a month.</td></tr></table>				Option	Description	daily	Upload log files to FortiAnalyzer once a day.	weekly	Upload log files to FortiAnalyzer once a week.	monthly	Upload log files to FortiAnalyzer once a month.		
Option	Description													
daily	Upload log files to FortiAnalyzer once a day.													
weekly	Upload log files to FortiAnalyzer once a week.													
monthly	Upload log files to FortiAnalyzer once a month.													
upload-option	Enable/disable logging to hard disk and then uploading to FortiAnalyzer.	option	-	5-minute										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>store-and-upload</td><td>Log to hard disk and then upload to FortiAnalyzer.</td></tr><tr><td>realtime</td><td>Log directly to FortiAnalyzer in real time.</td></tr><tr><td>1-minute</td><td>Log directly to FortiAnalyzer at least every 1 minute.</td></tr><tr><td>5-minute</td><td>Log directly to FortiAnalyzer at least every 5 minutes.</td></tr></table>				Option	Description	store-and-upload	Log to hard disk and then upload to FortiAnalyzer.	realtime	Log directly to FortiAnalyzer in real time.	1-minute	Log directly to FortiAnalyzer at least every 1 minute.	5-minute	Log directly to FortiAnalyzer at least every 5 minutes.
Option	Description													
store-and-upload	Log to hard disk and then upload to FortiAnalyzer.													
realtime	Log directly to FortiAnalyzer in real time.													
1-minute	Log directly to FortiAnalyzer at least every 1 minute.													
5-minute	Log directly to FortiAnalyzer at least every 5 minutes.													
upload-time	Time to upload logs (hh:mm).	user	Not Specified											

## config log fortiguard filter

Filters for FortiCloud.

```

config log fortiguard filter
    Description: Filters for FortiCloud.
    set anomaly [enable|disable]
    set forward-traffic [enable|disable]
    config free-style
        Description: Free style filters.
        edit <id>
            set category [traffic|event|...]
            set filter {string}
            set filter-type [include|exclude]
        next
    end
    set gtp [enable|disable]
    set local-traffic [enable|disable]
    set multicast-traffic [enable|disable]
    set severity [emergency|alert|...]
    set sniffer-traffic [enable|disable]
    set voip [enable|disable]
    set ztna-traffic [enable|disable]
end

```

## config log fortiguard filter

Parameter	Description	Type	Size	Default										
anomaly	Enable/disable anomaly logging.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable anomaly logging.</td></tr><tr><td><i>disable</i></td><td>Disable anomaly logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable anomaly logging.	<i>disable</i>	Disable anomaly logging.							
Option	Description													
<i>enable</i>	Enable anomaly logging.													
<i>disable</i>	Disable anomaly logging.													
forward-traffic	Enable/disable forward traffic logging.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable forward traffic logging.</td></tr><tr><td><i>disable</i></td><td>Disable forward traffic logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable forward traffic logging.	<i>disable</i>	Disable forward traffic logging.							
Option	Description													
<i>enable</i>	Enable forward traffic logging.													
<i>disable</i>	Disable forward traffic logging.													
gtp *	Enable/disable GTP messages logging.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable GTP messages logging.</td></tr><tr><td><i>disable</i></td><td>Disable GTP messages logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable GTP messages logging.	<i>disable</i>	Disable GTP messages logging.							
Option	Description													
<i>enable</i>	Enable GTP messages logging.													
<i>disable</i>	Disable GTP messages logging.													
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable local in or out traffic logging.</td></tr><tr><td><i>disable</i></td><td>Disable local in or out traffic logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable local in or out traffic logging.	<i>disable</i>	Disable local in or out traffic logging.							
Option	Description													
<i>enable</i>	Enable local in or out traffic logging.													
<i>disable</i>	Disable local in or out traffic logging.													
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable multicast traffic logging.</td></tr><tr><td><i>disable</i></td><td>Disable multicast traffic logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable multicast traffic logging.	<i>disable</i>	Disable multicast traffic logging.							
Option	Description													
<i>enable</i>	Enable multicast traffic logging.													
<i>disable</i>	Disable multicast traffic logging.													
severity	Lowest severity level to log.	option	-	information										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>emergency</i></td><td>Emergency level.</td></tr><tr><td><i>alert</i></td><td>Alert level.</td></tr><tr><td><i>critical</i></td><td>Critical level.</td></tr><tr><td><i>error</i></td><td>Error level.</td></tr></table>	Option	Description	<i>emergency</i>	Emergency level.	<i>alert</i>	Alert level.	<i>critical</i>	Critical level.	<i>error</i>	Error level.			
Option	Description													
<i>emergency</i>	Emergency level.													
<i>alert</i>	Alert level.													
<i>critical</i>	Critical level.													
<i>error</i>	Error level.													

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>warning</i>	Warning level.		
	<i>notification</i>	Notification level.		
	<i>information</i>	Information level.		
	<i>debug</i>	Debug level.		
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable sniffer traffic logging.		
	<i>disable</i>	Disable sniffer traffic logging.		
voip	Enable/disable VoIP logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable VoIP logging.		
	<i>disable</i>	Disable VoIP logging.		
ztna-traffic	Enable/disable ztna traffic logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable ztna traffic logging.		
	<i>disable</i>	Disable ztna traffic logging.		

\* This parameter may not exist in some models.

### config free-style

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
category	Log category.	option	-	traffic
	<b>Option</b>	<b>Description</b>		
	<i>traffic</i>	Traffic log.		

Parameter	Description	Type	Size	Default																																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>event</i></td><td>Event log.</td></tr><tr><td><i>virus</i></td><td>Antivirus log.</td></tr><tr><td><i>webfilter</i></td><td>Web filter log.</td></tr><tr><td><i>attack</i></td><td>Attack log.</td></tr><tr><td><i>spam</i></td><td>Antispam log.</td></tr><tr><td><i>anomaly</i></td><td>Anomaly log.</td></tr><tr><td><i>voip</i></td><td>VoIP log.</td></tr><tr><td><i>dlp</i></td><td>DLP log.</td></tr><tr><td><i>app-ctrl</i></td><td>Application control log.</td></tr><tr><td><i>waf</i></td><td>Web application firewall log.</td></tr><tr><td><i>dns</i></td><td>DNS detail log.</td></tr><tr><td><i>ssh</i></td><td>SSH log.</td></tr><tr><td><i>ssl</i></td><td>SSL log.</td></tr><tr><td><i>file-filter</i></td><td>File filter log.</td></tr><tr><td><i>icap</i></td><td>ICAP log.</td></tr></table>	Option	Description	<i>event</i>	Event log.	<i>virus</i>	Antivirus log.	<i>webfilter</i>	Web filter log.	<i>attack</i>	Attack log.	<i>spam</i>	Antispam log.	<i>anomaly</i>	Anomaly log.	<i>voip</i>	VoIP log.	<i>dlp</i>	DLP log.	<i>app-ctrl</i>	Application control log.	<i>waf</i>	Web application firewall log.	<i>dns</i>	DNS detail log.	<i>ssh</i>	SSH log.	<i>ssl</i>	SSL log.	<i>file-filter</i>	File filter log.	<i>icap</i>	ICAP log.			
	Option	Description																																		
	<i>event</i>	Event log.																																		
	<i>virus</i>	Antivirus log.																																		
	<i>webfilter</i>	Web filter log.																																		
	<i>attack</i>	Attack log.																																		
	<i>spam</i>	Antispam log.																																		
	<i>anomaly</i>	Anomaly log.																																		
	<i>voip</i>	VoIP log.																																		
	<i>dlp</i>	DLP log.																																		
	<i>app-ctrl</i>	Application control log.																																		
	<i>waf</i>	Web application firewall log.																																		
	<i>dns</i>	DNS detail log.																																		
	<i>ssh</i>	SSH log.																																		
	<i>ssl</i>	SSL log.																																		
	<i>file-filter</i>	File filter log.																																		
<i>icap</i>	ICAP log.																																			
filter	Free style filter string.	string	Maximum length: 1023																																	
filter-type	Include/exclude logs that match the filter.	option	-	include																																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>include</i></td><td>Include logs that match the filter.</td></tr><tr><td><i>exclude</i></td><td>Exclude logs that match the filter.</td></tr></table>	Option	Description	<i>include</i>	Include logs that match the filter.	<i>exclude</i>	Exclude logs that match the filter.																													
	Option	Description																																		
	<i>include</i>	Include logs that match the filter.																																		
<i>exclude</i>	Exclude logs that match the filter.																																			

## config log fortiguard override-filter

Override filters for FortiCloud.

```

config log fortiguard override-filter
  Description: Override filters for FortiCloud.
  set anomaly [enable|disable]
  set forward-traffic [enable|disable]
  config free-style
    Description: Free style filters.
    edit <id>
      set category [traffic|event|...]
      set filter {string}
    
```

```

        set filter-type [include|exclude]
    next
end
set gtp [enable|disable]
set local-traffic [enable|disable]
set multicast-traffic [enable|disable]
set severity [emergency|alert|...]
set sniffer-traffic [enable|disable]
set voip [enable|disable]
set ztna-traffic [enable|disable]
end

```

## config log fortiguard override-filter

Parameter	Description	Type	Size	Default						
anomaly	Enable/disable anomaly logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable anomaly logging.</td></tr><tr><td><i>disable</i></td><td>Disable anomaly logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable anomaly logging.	<i>disable</i>	Disable anomaly logging.			
Option	Description									
<i>enable</i>	Enable anomaly logging.									
<i>disable</i>	Disable anomaly logging.									
forward-traffic	Enable/disable forward traffic logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable forward traffic logging.</td></tr><tr><td><i>disable</i></td><td>Disable forward traffic logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable forward traffic logging.	<i>disable</i>	Disable forward traffic logging.			
Option	Description									
<i>enable</i>	Enable forward traffic logging.									
<i>disable</i>	Disable forward traffic logging.									
gtp *	Enable/disable GTP messages logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable GTP messages logging.</td></tr><tr><td><i>disable</i></td><td>Disable GTP messages logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable GTP messages logging.	<i>disable</i>	Disable GTP messages logging.			
Option	Description									
<i>enable</i>	Enable GTP messages logging.									
<i>disable</i>	Disable GTP messages logging.									
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable local in or out traffic logging.</td></tr><tr><td><i>disable</i></td><td>Disable local in or out traffic logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable local in or out traffic logging.	<i>disable</i>	Disable local in or out traffic logging.			
Option	Description									
<i>enable</i>	Enable local in or out traffic logging.									
<i>disable</i>	Disable local in or out traffic logging.									
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable multicast traffic logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable multicast traffic logging.					
Option	Description									
<i>enable</i>	Enable multicast traffic logging.									

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable multicast traffic logging.		
severity	Lowest severity level to log.	option	-	information
	<b>Option</b>	<b>Description</b>		
	<i>emergency</i>	Emergency level.		
	<i>alert</i>	Alert level.		
	<i>critical</i>	Critical level.		
	<i>error</i>	Error level.		
	<i>warning</i>	Warning level.		
	<i>notification</i>	Notification level.		
	<i>information</i>	Information level.		
	<i>debug</i>	Debug level.		
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable sniffer traffic logging.		
	<i>disable</i>	Disable sniffer traffic logging.		
voip	Enable/disable VoIP logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable VoIP logging.		
	<i>disable</i>	Disable VoIP logging.		
ztna-traffic	Enable/disable ztna traffic logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable ztna traffic logging.		
	<i>disable</i>	Disable ztna traffic logging.		

\* This parameter may not exist in some models.

## config free-style

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
category	Log category.	option	-	traffic
	<b>Option</b>	<b>Description</b>		
	<i>traffic</i>	Traffic log.		
	<i>event</i>	Event log.		
	<i>virus</i>	Antivirus log.		
	<i>webfilter</i>	Web filter log.		
	<i>attack</i>	Attack log.		
	<i>spam</i>	Antispam log.		
	<i>anomaly</i>	Anomaly log.		
	<i>voip</i>	VoIP log.		
	<i>dlp</i>	DLP log.		
	<i>app-ctrl</i>	Application control log.		
	<i>waf</i>	Web application firewall log.		
	<i>dns</i>	DNS detail log.		
	<i>ssh</i>	SSH log.		
	<i>ssl</i>	SSL log.		
	<i>file-filter</i>	File filter log.		
<i>icap</i>	ICAP log.			
filter	Free style filter string.	string	Maximum length: 1023	
filter-type	Include/exclude logs that match the filter.	option	-	include
	<b>Option</b>	<b>Description</b>		
	<i>include</i>	Include logs that match the filter.		
	<i>exclude</i>	Exclude logs that match the filter.		

## config log fortiguard override-setting

Override global FortiCloud logging settings for this VDOM.

```
config log fortiguard override-setting
  Description: Override global FortiCloud logging settings for this VDOM.
  set access-config [enable|disable]
  set max-log-rate {integer}
  set override [enable|disable]
  set priority [default|low]
  set status [enable|disable]
  set upload-day {user}
  set upload-interval [daily|weekly|...]
  set upload-option [store-and-upload|realtime|...]
  set upload-time {user}
end
```

## config log fortiguard override-setting

Parameter	Description	Type	Size	Default						
access-config	Enable/disable FortiCloud access to configuration and data.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable FortiCloud access to configuration and data.</td></tr><tr><td><i>disable</i></td><td>Disable FortiCloud access to configuration and data.</td></tr></table>	Option	Description	<i>enable</i>	Enable FortiCloud access to configuration and data.	<i>disable</i>	Disable FortiCloud access to configuration and data.			
Option	Description									
<i>enable</i>	Enable FortiCloud access to configuration and data.									
<i>disable</i>	Disable FortiCloud access to configuration and data.									
max-log-rate	FortiCloud maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0						
override	Overriding FortiCloud settings for this VDOM or use global settings.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Override FortiCloud logging settings.</td></tr><tr><td><i>disable</i></td><td>Use global FortiCloud logging settings.</td></tr></table>	Option	Description	<i>enable</i>	Override FortiCloud logging settings.	<i>disable</i>	Use global FortiCloud logging settings.			
Option	Description									
<i>enable</i>	Override FortiCloud logging settings.									
<i>disable</i>	Use global FortiCloud logging settings.									
priority	Set log transmission priority.	option	-	default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>Set FortiCloud log transmission priority to default.</td></tr><tr><td><i>low</i></td><td>Set FortiCloud log transmission priority to low.</td></tr></table>	Option	Description	<i>default</i>	Set FortiCloud log transmission priority to default.	<i>low</i>	Set FortiCloud log transmission priority to low.			
Option	Description									
<i>default</i>	Set FortiCloud log transmission priority to default.									
<i>low</i>	Set FortiCloud log transmission priority to low.									
status	Enable/disable logging to FortiCloud.	option	-	disable						



Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable logging to FortiCloud.		
	<i>disable</i>	Disable logging to FortiCloud.		
upload-day	Day of week to roll logs.	user	Not Specified	
upload-interval	Frequency of uploading log files to FortiCloud.	option	-	daily
	<b>Option</b>	<b>Description</b>		
	<i>daily</i>	Upload log files to FortiCloud once a day.		
	<i>weekly</i>	Upload log files to FortiCloud once a week.		
	<i>monthly</i>	Upload log files to FortiCloud once a month.		
upload-option	Configure how log messages are sent to FortiCloud.	option	-	5-minute
	<b>Option</b>	<b>Description</b>		
	<i>store-and-upload</i>	Log to the hard disk and then upload logs to FortiCloud.		
	<i>realtime</i>	Log directly to FortiCloud in real time.		
	<i>1-minute</i>	Log directly to FortiCloud at 1-minute intervals.		
	<i>5-minute</i>	Log directly to FortiCloud at 5-minute intervals.		
upload-time	Time of day to roll logs (hh:mm).	user	Not Specified	

## config log fortiguard setting

Configure logging to FortiCloud.

```
config log fortiguard setting
  Description: Configure logging to FortiCloud.
  set access-config [enable|disable]
  set conn-timeout {integer}
  set enc-algorithm [high-medium|high|...]
  set interface {string}
  set interface-select-method [auto|sdwan|...]
  set max-log-rate {integer}
  set priority [default|low]
  set source-ip {ipv4-address}
  set ssl-min-proto-version [default|SSLv3|...]
  set status [enable|disable]
  set upload-day {user}
  set upload-interval [daily|weekly|...]
  set upload-option [store-and-upload|realtime|...]
```

```

set upload-time {user}
end

```

## config log fortiguard setting

Parameter	Description	Type	Size	Default
access-config	Enable/disable FortiCloud access to configuration and data.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable FortiCloud access to configuration and data.		
	<i>disable</i>	Disable FortiCloud access to configuration and data.		
conn-timeout	FortiGate Cloud connection timeout in seconds.	integer	Minimum value: 1 Maximum value: 3600	10
enc-algorithm	Configure the level of SSL protection for secure communication with FortiCloud.	option	-	high
	<b>Option</b>	<b>Description</b>		
	<i>high-medium</i>	Encrypt logs using high and medium encryption.		
	<i>high</i>	Encrypt logs using high encryption.		
	<i>low</i>	Encrypt logs using low encryption.		
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto
	<b>Option</b>	<b>Description</b>		
	<i>auto</i>	Set outgoing interface automatically.		
	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.		
	<i>specify</i>	Set outgoing interface manually.		
max-log-rate	FortiCloud maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0
priority	Set log transmission priority.	option	-	default

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>default</i>	Set FortiCloud log transmission priority to default.		
	<i>low</i>	Set FortiCloud log transmission priority to low.		
source-ip	Source IP address used to connect FortiCloud.	ipv4-address	Not Specified	0.0.0.0
ssl-min-protocol-version	Minimum supported protocol version for SSL/TLS connections.	option	-	default
	<b>Option</b>	<b>Description</b>		
	<i>default</i>	Follow system global setting.		
	<i>SSLv3</i>	SSLv3.		
	<i>TLSv1</i>	TLSv1.		
	<i>TLSv1-1</i>	TLSv1.1.		
	<i>TLSv1-2</i>	TLSv1.2.		
status	Enable/disable logging to FortiCloud.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable logging to FortiCloud.		
	<i>disable</i>	Disable logging to FortiCloud.		
upload-day	Day of week to roll logs.	user	Not Specified	
upload-interval	Frequency of uploading log files to FortiCloud.	option	-	daily
	<b>Option</b>	<b>Description</b>		
	<i>daily</i>	Upload log files to FortiCloud once a day.		
	<i>weekly</i>	Upload log files to FortiCloud once a week.		
	<i>monthly</i>	Upload log files to FortiCloud once a month.		
upload-option	Configure how log messages are sent to FortiCloud.	option	-	5-minute
	<b>Option</b>	<b>Description</b>		
	<i>store-and-upload</i>	Log to the hard disk and then upload logs to FortiCloud.		
	<i>realtime</i>	Log directly to FortiCloud in real time.		

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>1-minute</i>	Log directly to FortiCloud at 1-minute intervals.		
	<i>5-minute</i>	Log directly to FortiCloud at 5-minute intervals.		
upload-time	Time of day to roll logs (hh:mm).	user	Not Specified	

## config log gui-display

Configure how log messages are displayed on the GUI.

```
config log gui-display
    Description: Configure how log messages are displayed on the GUI.
    set fortiview-unscanned-apps [enable|disable]
    set resolve-apps [enable|disable]
    set resolve-hosts [enable|disable]
end
```

## config log gui-display

Parameter	Description	Type	Size	Default
fortiview-unscanned-apps	Enable/disable showing unscanned traffic in FortiView application charts.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable showing unscanned traffic.		
	<i>disable</i>	Disable showing unscanned traffic.		
resolve-apps	Resolve unknown applications on the GUI using Fortinet's remote application database.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable unknown applications on the GUI.		
	<i>disable</i>	Disable unknown applications on the GUI.		
resolve-hosts	Enable/disable resolving IP addresses to hostname in log messages on the GUI using reverse DNS lookup.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable resolving IP addresses to hostnames.		
	<i>disable</i>	Disable resolving IP addresses to hostnames.		

## config log memory filter

Filters for memory buffer.

```
config log memory filter
  Description: Filters for memory buffer.
  set anomaly [enable|disable]
  set forward-traffic [enable|disable]
  config free-style
    Description: Free style filters.
    edit <id>
      set category [traffic|event|...]
      set filter {string}
      set filter-type [include|exclude]
    next
  end
  set gtp [enable|disable]
  set local-traffic [enable|disable]
  set multicast-traffic [enable|disable]
  set severity [emergency|alert|...]
  set sniffer-traffic [enable|disable]
  set voip [enable|disable]
  set ztna-traffic [enable|disable]
end
```

## config log memory filter

Parameter	Description	Type	Size	Default
anomaly	Enable/disable anomaly logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable anomaly logging.		
	<i>disable</i>	Disable anomaly logging.		
forward-traffic	Enable/disable forward traffic logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable forward traffic logging.		
	<i>disable</i>	Disable forward traffic logging.		
gtp *	Enable/disable GTP messages logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable GTP messages logging.		
	<i>disable</i>	Disable GTP messages logging.		
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable **

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable local in or out traffic logging.		
	<i>disable</i>	Disable local in or out traffic logging.		
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable multicast traffic logging.		
	<i>disable</i>	Disable multicast traffic logging.		
severity	Log every message above and including this severity level.	option	-	information
	<b>Option</b>	<b>Description</b>		
	<i>emergency</i>	Emergency level.		
	<i>alert</i>	Alert level.		
	<i>critical</i>	Critical level.		
	<i>error</i>	Error level.		
	<i>warning</i>	Warning level.		
	<i>notification</i>	Notification level.		
	<i>information</i>	Information level.		
	<i>debug</i>	Debug level.		
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable sniffer traffic logging.		
	<i>disable</i>	Disable sniffer traffic logging.		
voip	Enable/disable VoIP logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable VoIP logging.		
	<i>disable</i>	Disable VoIP logging.		
ztina-traffic	Enable/disable ztna traffic logging.	option	-	enable

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable ztna traffic logging.		
	<i>disable</i>	Disable ztna traffic logging.		

\* This parameter may not exist in some models.

\*\* Values may differ between models.

### config free-style

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
category	Log category.	option	-	traffic
	<b>Option</b>	<b>Description</b>		
	<i>traffic</i>	Traffic log.		
	<i>event</i>	Event log.		
	<i>virus</i>	Antivirus log.		
	<i>webfilter</i>	Web filter log.		
	<i>attack</i>	Attack log.		
	<i>spam</i>	Antispam log.		
	<i>anomaly</i>	Anomaly log.		
	<i>voip</i>	VoIP log.		
	<i>dlp</i>	DLP log.		
	<i>app-ctrl</i>	Application control log.		
	<i>waf</i>	Web application firewall log.		
	<i>dns</i>	DNS detail log.		
	<i>ssh</i>	SSH log.		
	<i>ssl</i>	SSL log.		
	<i>file-filter</i>	File filter log.		
	<i>icap</i>	ICAP log.		

Parameter	Description	Type	Size	Default						
filter	Free style filter string.	string	Maximum length: 1023							
filter-type	Include/exclude logs that match the filter.	option	-	include						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>include</i></td><td>Include logs that match the filter.</td></tr><tr><td><i>exclude</i></td><td>Exclude logs that match the filter.</td></tr></table>				Option	Description	<i>include</i>	Include logs that match the filter.	<i>exclude</i>	Exclude logs that match the filter.
Option	Description									
<i>include</i>	Include logs that match the filter.									
<i>exclude</i>	Exclude logs that match the filter.									

## config log memory global-setting

Global settings for memory logging.

```
config log memory global-setting
    Description: Global settings for memory logging.
    set full-final-warning-threshold {integer}
    set full-first-warning-threshold {integer}
    set full-second-warning-threshold {integer}
    set max-size {integer}
end
```

## config log memory global-setting

Parameter	Description	Type	Size	Default
full-final-warning-threshold	Log full final warning threshold as a percent.	integer	Minimum value: 3 Maximum value: 100	95
full-first-warning-threshold	Log full first warning threshold as a percent.	integer	Minimum value: 1 Maximum value: 98	75
full-second-warning-threshold	Log full second warning threshold as a percent.	integer	Minimum value: 2 Maximum value: 99	90
max-size	Maximum amount of memory that can be used for memory logging in bytes.	integer	Minimum value: 0 Maximum value: 4294967295	168440954 **

\*\* Values may differ between models.



## config log memory setting

Settings for memory buffer.

```
config log memory setting
    Description: Settings for memory buffer.
    set status [enable|disable]
end
```

## config log memory setting

Parameter	Description	Type	Size	Default
status	Enable/disable logging to the FortiGate's memory.	option	-	enable **
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable logging to memory.		
	<i>disable</i>	Disable logging to memory.		

\*\* Values may differ between models.

## config log npu-server



This command is available for model(s): FortiGate 2600F.

It is not available for: FortiGate 1000D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

Configure all the log servers and create the server groups.

```

config log npu-server
    Description: Configure all the log servers and create the server groups.
    set log-processor [hardware|host]
    set log-processing [may-drop|no-drop]
    set netflow-ver [v9|v10]
    set syslog-facility {integer}
    set syslog-severity {integer}
    config server-info
        Description: configure server info.
        edit <id>
            set vdom {string}
            set ip-family [v4|v6]
            set ipv4-server {ipv4-address-any}
            set ipv6-server {ipv6-address}
            set source-port {integer}
            set dest-port {integer}
            set template-tx-timeout {integer}
        next
    end
    config server-group
        Description: create server group.
        edit <group-name>
            set log-mode [per-session|per-nat-mapping|...]
            set log-format [syslog|netflow]
            set log-user-info [disable|enable]
            set log-gen-event [disable|enable]
            set log-tx-mode [roundrobin|multicast]
            set sw-log-flags [tcp-udp-only|enable-all-log|...]
            set server-number {integer}
            set server-start-id {integer}
        next
    end
end

```

## config log npu-server

Parameter	Description	Type	Size	Default						
log-processor	configure the log module.	option	-	hardware						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>hardware</i></td><td>Hardware handles the log processing.</td></tr><tr><td><i>host</i></td><td>Host handles the log processing.</td></tr></table>	Option	Description	<i>hardware</i>	Hardware handles the log processing.	<i>host</i>	Host handles the log processing.			
Option	Description									
<i>hardware</i>	Hardware handles the log processing.									
<i>host</i>	Host handles the log processing.									
log-processing	configure log processed by host to drop or no drop.	option	-	no-drop						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>may-drop</i></td><td>Log processed by host may drop</td></tr><tr><td><i>no-drop</i></td><td>Log processed by host may not drop</td></tr></table>	Option	Description	<i>may-drop</i>	Log processed by host may drop	<i>no-drop</i>	Log processed by host may not drop			
Option	Description									
<i>may-drop</i>	Log processed by host may drop									
<i>no-drop</i>	Log processed by host may not drop									

Parameter	Description	Type	Size	Default						
netflow-ver	configure the netflow version.	option	-	v10						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>v9</td><td>Netflow v9.</td></tr><tr><td>v10</td><td>Netflow v10, that is IPFIX.</td></tr></table>	Option	Description	v9	Netflow v9.	v10	Netflow v10, that is IPFIX.			
Option	Description									
v9	Netflow v9.									
v10	Netflow v10, that is IPFIX.									
syslog-facility	configure the syslog facility.	integer	Minimum value: 0 Maximum value: 255	23						
syslog-severity	configure the syslog severity.	integer	Minimum value: 0 Maximum value: 255	5						

### config server-info

Parameter	Description	Type	Size	Default						
id	server id.	integer	Minimum value: 1 Maximum value: 16	0						
vdom	Interface connected to the log server is in this virtual domain (VDOM).	string	Maximum length: 31							
ip-family	set the version the IP address	option	-	v4						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>v4</td><td>IP v4.</td></tr><tr><td>v6</td><td>IP v6.</td></tr></table>				Option	Description	v4	IP v4.	v6	IP v6.
	Option	Description								
	v4	IP v4.								
v6	IP v6.									
ipv4-server	set the IPv4 address for the log server	ipv4-address-any	Not Specified	0.0.0.0						
ipv6-server	set the IPv6 address for the log server	ipv6-address	Not Specified	::						
source-port	set the source port for the log packet	integer	Minimum value: 0 Maximum value: 65535	0						

Parameter	Description	Type	Size	Default
dest-port	set the dest port for the log packet	integer	Minimum value: 0 Maximum value: 65535	0
template-tx-timeout	set the template tx timeout	integer	Minimum value: 60 Maximum value: 86400	600

### config server-group

Parameter	Description	Type	Size	Default								
group-name	server group name.	string	Maximum length: 35									
log-mode	Set the log mode	option	-	per-session								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>per-session</i></td><td>Create log when setup and delete session.</td></tr><tr><td><i>per-nat-mapping</i></td><td>Create log when allocate or free mapping resource.</td></tr><tr><td><i>per-session-ending</i></td><td>Create log only when delete session.</td></tr></table>	Option	Description	<i>per-session</i>	Create log when setup and delete session.	<i>per-nat-mapping</i>	Create log when allocate or free mapping resource.	<i>per-session-ending</i>	Create log only when delete session.			
Option	Description											
<i>per-session</i>	Create log when setup and delete session.											
<i>per-nat-mapping</i>	Create log when allocate or free mapping resource.											
<i>per-session-ending</i>	Create log only when delete session.											
log-format	Set the log format	option	-	netflow								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>syslog</i></td><td>Create the log in the format of syslog.</td></tr><tr><td><i>netflow</i></td><td>Create the log in the format of netflow, the netflow version is v9 or v10, depends on the netflow_ver set.</td></tr></table>	Option	Description	<i>syslog</i>	Create the log in the format of syslog.	<i>netflow</i>	Create the log in the format of netflow, the netflow version is v9 or v10, depends on the netflow_ver set.					
Option	Description											
<i>syslog</i>	Create the log in the format of syslog.											
<i>netflow</i>	Create the log in the format of netflow, the netflow version is v9 or v10, depends on the netflow_ver set.											
log-user-info	Enable/disbale logging user information.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Do not log user informaton in logs.</td></tr><tr><td><i>enable</i></td><td>Log user information in logs.</td></tr></table>	Option	Description	<i>disable</i>	Do not log user informaton in logs.	<i>enable</i>	Log user information in logs.					
Option	Description											
<i>disable</i>	Do not log user informaton in logs.											
<i>enable</i>	Log user information in logs.											
log-gen-event	Enable/disbale generating event for Per-Mapping log	option	-	disable								

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Do not generate system event for per-mapping logs.		
	<i>enable</i>	Generate system event for per-mapping logs.		
log-tx-mode	Configure log transmit mode.	option	-	roundrobin
	<b>Option</b>	<b>Description</b>		
	<i>roundrobin</i>	Transmit logs in round-robin mode.		
	<i>multicast</i>	Transmit logs in multicast mode.		
sw-log-flags	Set flags for software logging via driver.	option	-	tcp-udp-only
	<b>Option</b>	<b>Description</b>		
	<i>tcp-udp-only</i>	Only TCP/UDP software sessions are logged. (default)		
	<i>enable-all-log</i>	All protocols of software sessions are logged.		
	<i>disable-all-log</i>	No software sessions are logged.		
server-number	server number in this group.	integer	Minimum value: 1 Maximum value: 16	1
server-start-id	the start id of the continuous server series in this group, [1,16].	integer	Minimum value: 1 Maximum value: 16	0

## config log null-device filter

Filters for null device logging.

```

config log null-device filter
    Description: Filters for null device logging.
    set anomaly [enable|disable]
    set forward-traffic [enable|disable]
    config free-style
        Description: Free style filters.
        edit <id>
            set category [traffic|event|...]
            set filter {string}
            set filter-type [include|exclude]
        next
    end
    set gtp [enable|disable]
    set local-traffic [enable|disable]
    set multicast-traffic [enable|disable]

```

```

set severity [emergency|alert|...]
set sniffer-traffic [enable|disable]
set voip [enable|disable]
set ztna-traffic [enable|disable]
end

```

## config log null-device filter

Parameter	Description	Type	Size	Default
anomaly	Enable/disable anomaly logging.	option	-	enable
	Option	Description		
	enable	Enable anomaly logging.		
	disable	Disable anomaly logging.		
forward-traffic	Enable/disable forward traffic logging.	option	-	enable
	Option	Description		
	enable	Enable forward traffic logging.		
	disable	Disable forward traffic logging.		
gtp *	Enable/disable GTP messages logging.	option	-	enable
	Option	Description		
	enable	Enable GTP messages logging.		
	disable	Disable GTP messages logging.		
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable
	Option	Description		
	enable	Enable local in or out traffic logging.		
	disable	Disable local in or out traffic logging.		
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable
	Option	Description		
	enable	Enable multicast traffic logging.		
	disable	Disable multicast traffic logging.		
severity	Lowest severity level to log.	option	-	information

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>emergency</i>	Emergency level.		
	<i>alert</i>	Alert level.		
	<i>critical</i>	Critical level.		
	<i>error</i>	Error level.		
	<i>warning</i>	Warning level.		
	<i>notification</i>	Notification level.		
	<i>information</i>	Information level.		
	<i>debug</i>	Debug level.		
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable sniffer traffic logging.		
	<i>disable</i>	Disable sniffer traffic logging.		
voip	Enable/disable VoIP logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable VoIP logging.		
	<i>disable</i>	Disable VoIP logging.		
ztna-traffic	Enable/disable ztna traffic logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable ztna traffic logging.		
	<i>disable</i>	Disable ztna traffic logging.		

\* This parameter may not exist in some models.

### config free-style

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0

Parameter	Description	Type	Size	Default																																			
category	Log category.	option	-	traffic																																			
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>traffic</td><td>Traffic log.</td></tr><tr><td>event</td><td>Event log.</td></tr><tr><td>virus</td><td>Antivirus log.</td></tr><tr><td>webfilter</td><td>Web filter log.</td></tr><tr><td>attack</td><td>Attack log.</td></tr><tr><td>spam</td><td>Antispam log.</td></tr><tr><td>anomaly</td><td>Anomaly log.</td></tr><tr><td>voip</td><td>VoIP log.</td></tr><tr><td>dlp</td><td>DLP log.</td></tr><tr><td>app-ctrl</td><td>Application control log.</td></tr><tr><td>waf</td><td>Web application firewall log.</td></tr><tr><td>dns</td><td>DNS detail log.</td></tr><tr><td>ssh</td><td>SSH log.</td></tr><tr><td>ssl</td><td>SSL log.</td></tr><tr><td>file-filter</td><td>File filter log.</td></tr><tr><td>icap</td><td>ICAP log.</td></tr></table>	Option	Description	traffic	Traffic log.	event	Event log.	virus	Antivirus log.	webfilter	Web filter log.	attack	Attack log.	spam	Antispam log.	anomaly	Anomaly log.	voip	VoIP log.	dlp	DLP log.	app-ctrl	Application control log.	waf	Web application firewall log.	dns	DNS detail log.	ssh	SSH log.	ssl	SSL log.	file-filter	File filter log.	icap	ICAP log.				
	Option	Description																																					
	traffic	Traffic log.																																					
	event	Event log.																																					
	virus	Antivirus log.																																					
	webfilter	Web filter log.																																					
	attack	Attack log.																																					
	spam	Antispam log.																																					
	anomaly	Anomaly log.																																					
	voip	VoIP log.																																					
	dlp	DLP log.																																					
	app-ctrl	Application control log.																																					
	waf	Web application firewall log.																																					
	dns	DNS detail log.																																					
	ssh	SSH log.																																					
	ssl	SSL log.																																					
	file-filter	File filter log.																																					
icap	ICAP log.																																						
filter	Free style filter string.	string	Maximum length: 1023																																				
filter-type	Include/exclude logs that match the filter.	option	-	include																																			
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>include</td><td>Include logs that match the filter.</td></tr><tr><td>exclude</td><td>Exclude logs that match the filter.</td></tr></table>	Option	Description	include	Include logs that match the filter.	exclude	Exclude logs that match the filter.																																
	Option	Description																																					
	include	Include logs that match the filter.																																					
exclude	Exclude logs that match the filter.																																						

## config log null-device setting

Settings for null device logging.

```

config log null-device setting
    Description: Settings for null device logging.
    set status [enable|disable]
end

```



## config log null-device setting

Parameter	Description	Type	Size	Default
status	Enable/disable statistics collection for when no external logging destination, such as FortiAnalyzer, is present (data is not saved).	option	-	disable
	Option	Description		
	<i>enable</i>	Enable statistics collection for when no external logging destination, such as FortiAnalyzer, is present (data is not saved).		
	<i>disable</i>	Disable statistics collection for when no external logging destination, such as FortiAnalyzer, is present (data is not saved).		

## config log setting

Configure general log settings.

```
config log setting
    Description: Configure general log settings.
    set anonymization-hash {string}
    set brief-traffic-format [enable|disable]
    set custom-log-fields <field-id1>, <field-id2>, ...
    set daemon-log [enable|disable]
    set expolicy-implicit-log [enable|disable]
    set faz-override [enable|disable]
    set fortiview-weekly-data [enable|disable]
    set fwpolicy-implicit-log [enable|disable]
    set fwpolicy6-implicit-log [enable|disable]
    set local-in-allow [enable|disable]
    set local-in-deny-broadcast [enable|disable]
    set local-in-deny-unicast [enable|disable]
    set local-out [enable|disable]
    set log-invalid-packet [enable|disable]
    set log-policy-comment [enable|disable]
    set log-user-in-upper [enable|disable]
    set neighbor-event [enable|disable]
    set resolve-ip [enable|disable]
    set resolve-port [enable|disable]
    set rest-api-get [enable|disable]
    set rest-api-set [enable|disable]
    set syslog-override [enable|disable]
    set user-anonymize [enable|disable]
end
```

## config log setting

Parameter	Description	Type	Size	Default
anonymization-hash	User name anonymization hash salt.	string	Maximum length: 32	
brief-traffic-format	Enable/disable brief format traffic logging.	option	-	disable
	Option	Description		
	enable	Enable brief format traffic logging.		
	disable	Disable brief format traffic logging.		
custom-log-fields <field-id>	Custom fields to append to all log messages. Custom log field.	string	Maximum length: 35	
daemon-log	Enable/disable daemon logging.	option	-	disable
	Option	Description		
	enable	Enable daemon logging.		
	disable	Disable daemon logging.		
expolicy-implicit-log	Enable/disable explicit proxy firewall implicit policy logging.	option	-	disable
	Option	Description		
	enable	Enable explicit proxy firewall implicit policy logging.		
	disable	Disable explicit proxy firewall implicit policy logging.		
faz-override	Enable/disable override FortiAnalyzer settings.	option	-	disable
	Option	Description		
	enable	Enable override FortiAnalyzer settings.		
	disable	Disable override FortiAnalyzer settings.		
fortiview-weekly-data *	Enable/disable FortiView weekly data.	option	-	disable
	Option	Description		
	enable	Enable FortiView weekly data.		
	disable	Disable FortiView weekly data.		
fwpolicy-implicit-log	Enable/disable implicit firewall policy logging.	option	-	disable

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable implicit firewall policy logging.		
	<i>disable</i>	Disable implicit firewall policy logging.		
fwpolicy6-implicit-log	Enable/disable implicit firewall policy6 logging.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable implicit firewall policy6 logging.		
	<i>disable</i>	Disable implicit firewall policy6 logging.		
local-in-allow	Enable/disable local-in-allow logging.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable local-in-allow logging.		
	<i>disable</i>	Disable local-in-allow logging.		
local-in-deny-broadcast	Enable/disable local-in-deny-broadcast logging.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable local-in-deny-broadcast logging.		
	<i>disable</i>	Disable local-in-deny-broadcast logging.		
local-in-deny-unicast	Enable/disable local-in-deny-unicast logging.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable local-in-deny-unicast logging.		
	<i>disable</i>	Disable local-in-deny-unicast logging.		
local-out	Enable/disable local-out logging.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable local-out logging.		
	<i>disable</i>	Disable local-out logging.		
log-invalid-packet	Enable/disable invalid packet traffic logging.	option	-	disable

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable invalid packet traffic logging.		
	<i>disable</i>	Disable invalid packet traffic logging.		
log-policy-comment	Enable/disable inserting policy comments into traffic logs.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable inserting policy comments into traffic logs.		
	<i>disable</i>	Disable inserting policy comments into traffic logs.		
log-user-in-upper	Enable/disable logs with user-in-upper.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable logs with user-in-upper.		
	<i>disable</i>	Disable logs with user-in-upper.		
neighbor-event	Enable/disable neighbor event logging.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable neighbor event logging.		
	<i>disable</i>	Disable neighbor event logging.		
resolve-ip	Enable/disable adding resolved domain names to traffic logs if possible.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable adding resolved domain names to traffic logs.		
	<i>disable</i>	Disable adding resolved domain names to traffic logs.		
resolve-port	Enable/disable adding resolved service names to traffic logs.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable adding resolved service names to traffic logs.		
	<i>disable</i>	Disable adding resolved service names to traffic logs.		
rest-api-get	Enable/disable REST API GET request logging.	option	-	disable

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable GET REST API logging.		
	<i>disable</i>	Disable GET REST API logging.		
rest-api-set	Enable/disable REST API POST/PUT/DELETE request logging.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable POST/PUT/DELETE REST API logging.		
	<i>disable</i>	Disable POST/PUT/DELETE REST API logging.		
syslog-override	Enable/disable override Syslog settings.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable override Syslog settings.		
	<i>disable</i>	Disable override Syslog settings.		
user-anonymize	Enable/disable anonymizing user names in log messages.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable anonymizing user names in log messages.		
	<i>disable</i>	Disable anonymizing user names in log messages.		

\* This parameter may not exist in some models.

## config log syslogd2 filter

Filters for remote system server.

```
config log syslogd2 filter
    Description: Filters for remote system server.
    set anomaly [enable|disable]
    set forward-traffic [enable|disable]
    config free-style
        Description: Free style filters.
        edit <id>
            set category [traffic|event|...]
            set filter {string}
            set filter-type [include|exclude]
        next
    end
    set gtp [enable|disable]
    set local-traffic [enable|disable]
    set multicast-traffic [enable|disable]
```

```

set severity [emergency|alert|...]
set sniffer-traffic [enable|disable]
set voip [enable|disable]
set ztna-traffic [enable|disable]
end

```

## config log syslogd2 filter

Parameter	Description	Type	Size	Default
anomaly	Enable/disable anomaly logging.	option	-	enable
	Option	Description		
	enable	Enable anomaly logging.		
	disable	Disable anomaly logging.		
forward-traffic	Enable/disable forward traffic logging.	option	-	enable
	Option	Description		
	enable	Enable forward traffic logging.		
	disable	Disable forward traffic logging.		
gtp *	Enable/disable GTP messages logging.	option	-	enable
	Option	Description		
	enable	Enable GTP messages logging.		
	disable	Disable GTP messages logging.		
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable
	Option	Description		
	enable	Enable local in or out traffic logging.		
	disable	Disable local in or out traffic logging.		
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable
	Option	Description		
	enable	Enable multicast traffic logging.		
	disable	Disable multicast traffic logging.		
severity	Lowest severity level to log.	option	-	information

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>emergency</i>	Emergency level.		
	<i>alert</i>	Alert level.		
	<i>critical</i>	Critical level.		
	<i>error</i>	Error level.		
	<i>warning</i>	Warning level.		
	<i>notification</i>	Notification level.		
	<i>information</i>	Information level.		
	<i>debug</i>	Debug level.		
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable sniffer traffic logging.		
	<i>disable</i>	Disable sniffer traffic logging.		
voip	Enable/disable VoIP logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable VoIP logging.		
	<i>disable</i>	Disable VoIP logging.		
ztna-traffic	Enable/disable ztna traffic logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable ztna traffic logging.		
	<i>disable</i>	Disable ztna traffic logging.		

\* This parameter may not exist in some models.

### config free-style

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0

Parameter	Description	Type	Size	Default																																		
category	Log category.	option	-	traffic																																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>traffic</td><td>Traffic log.</td></tr><tr><td>event</td><td>Event log.</td></tr><tr><td>virus</td><td>Antivirus log.</td></tr><tr><td>webfilter</td><td>Web filter log.</td></tr><tr><td>attack</td><td>Attack log.</td></tr><tr><td>spam</td><td>Antispam log.</td></tr><tr><td>anomaly</td><td>Anomaly log.</td></tr><tr><td>voip</td><td>VoIP log.</td></tr><tr><td>dlp</td><td>DLP log.</td></tr><tr><td>app-ctrl</td><td>Application control log.</td></tr><tr><td>waf</td><td>Web application firewall log.</td></tr><tr><td>dns</td><td>DNS detail log.</td></tr><tr><td>ssh</td><td>SSH log.</td></tr><tr><td>ssl</td><td>SSL log.</td></tr><tr><td>file-filter</td><td>File filter log.</td></tr><tr><td>icap</td><td>ICAP log.</td></tr></table>	Option	Description	traffic	Traffic log.	event	Event log.	virus	Antivirus log.	webfilter	Web filter log.	attack	Attack log.	spam	Antispam log.	anomaly	Anomaly log.	voip	VoIP log.	dlp	DLP log.	app-ctrl	Application control log.	waf	Web application firewall log.	dns	DNS detail log.	ssh	SSH log.	ssl	SSL log.	file-filter	File filter log.	icap	ICAP log.			
	Option	Description																																				
	traffic	Traffic log.																																				
	event	Event log.																																				
	virus	Antivirus log.																																				
	webfilter	Web filter log.																																				
	attack	Attack log.																																				
	spam	Antispam log.																																				
	anomaly	Anomaly log.																																				
	voip	VoIP log.																																				
	dlp	DLP log.																																				
	app-ctrl	Application control log.																																				
	waf	Web application firewall log.																																				
	dns	DNS detail log.																																				
	ssh	SSH log.																																				
	ssl	SSL log.																																				
	file-filter	File filter log.																																				
icap	ICAP log.																																					
filter	Free style filter string.	string	Maximum length: 1023																																			
filter-type	Include/exclude logs that match the filter.	option	-	include																																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>include</td><td>Include logs that match the filter.</td></tr><tr><td>exclude</td><td>Exclude logs that match the filter.</td></tr></table>	Option	Description	include	Include logs that match the filter.	exclude	Exclude logs that match the filter.																															
	Option	Description																																				
	include	Include logs that match the filter.																																				
exclude	Exclude logs that match the filter.																																					

## config log syslogd2 override-filter

Override filters for remote system server.

```
config log syslogd2 override-filter
  Description: Override filters for remote system server.
  set anomaly [enable|disable]
  set forward-traffic [enable|disable]
  config free-style
    Description: Free style filters.
```



```

edit <id>
    set category [traffic|event|...]
    set filter {string}
    set filter-type [include|exclude]
next
end
set gtp [enable|disable]
set local-traffic [enable|disable]
set multicast-traffic [enable|disable]
set severity [emergency|alert|...]
set sniffer-traffic [enable|disable]
set voip [enable|disable]
set ztna-traffic [enable|disable]
end

```

## config log syslogd2 override-filter

Parameter	Description	Type	Size	Default
anomaly	Enable/disable anomaly logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable anomaly logging.		
	<i>disable</i>	Disable anomaly logging.		
forward-traffic	Enable/disable forward traffic logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable forward traffic logging.		
	<i>disable</i>	Disable forward traffic logging.		
gtp *	Enable/disable GTP messages logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable GTP messages logging.		
	<i>disable</i>	Disable GTP messages logging.		
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable local in or out traffic logging.		
	<i>disable</i>	Disable local in or out traffic logging.		
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable multicast traffic logging.		
	<i>disable</i>	Disable multicast traffic logging.		
severity	Lowest severity level to log.	option	-	information
	<b>Option</b>	<b>Description</b>		
	<i>emergency</i>	Emergency level.		
	<i>alert</i>	Alert level.		
	<i>critical</i>	Critical level.		
	<i>error</i>	Error level.		
	<i>warning</i>	Warning level.		
	<i>notification</i>	Notification level.		
	<i>information</i>	Information level.		
	<i>debug</i>	Debug level.		
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable sniffer traffic logging.		
	<i>disable</i>	Disable sniffer traffic logging.		
voip	Enable/disable VoIP logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable VoIP logging.		
	<i>disable</i>	Disable VoIP logging.		
ztna-traffic	Enable/disable ztna traffic logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable ztna traffic logging.		
	<i>disable</i>	Disable ztna traffic logging.		

\* This parameter may not exist in some models.

## config free-style

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
category	Log category.	option	-	traffic
	<b>Option</b>	<b>Description</b>		
	<i>traffic</i>	Traffic log.		
	<i>event</i>	Event log.		
	<i>virus</i>	Antivirus log.		
	<i>webfilter</i>	Web filter log.		
	<i>attack</i>	Attack log.		
	<i>spam</i>	Antispam log.		
	<i>anomaly</i>	Anomaly log.		
	<i>voip</i>	VoIP log.		
	<i>dlp</i>	DLP log.		
	<i>app-ctrl</i>	Application control log.		
	<i>waf</i>	Web application firewall log.		
	<i>dns</i>	DNS detail log.		
	<i>ssh</i>	SSH log.		
	<i>ssl</i>	SSL log.		
	<i>file-filter</i>	File filter log.		
<i>icap</i>	ICAP log.			
filter	Free style filter string.	string	Maximum length: 1023	
filter-type	Include/exclude logs that match the filter.	option	-	include
	<b>Option</b>	<b>Description</b>		
	<i>include</i>	Include logs that match the filter.		
	<i>exclude</i>	Exclude logs that match the filter.		

## config log syslogd2 override-setting

Override settings for remote syslog server.

```
config log syslogd2 override-setting
  Description: Override settings for remote syslog server.
  set certificate {string}
  config custom-field-name
    Description: Custom field name for CEF format logging.
    edit <id>
      set name {string}
      set custom {string}
    next
  end
  set enc-algorithm [high-medium|high|...]
  set facility [kernel|user|...]
  set format [default|csv|...]
  set interface {string}
  set interface-select-method [auto|sdwan|...]
  set max-log-rate {integer}
  set mode [udp|legacy-reliable|...]
  set port {integer}
  set priority [default|low]
  set server {string}
  set source-ip {string}
  set ssl-min-proto-version [default|SSLv3|...]
  set status [enable|disable]
end
```

## config log syslogd2 override-setting

Parameter	Description	Type	Size	Default
certificate	Certificate used to communicate with Syslog server.	string	Maximum length: 35	
enc-algorithm	Enable/disable reliable syslogging with TLS encryption.	option	-	disable
	<div><div>Option</div><div>Description</div></div>			
	high-medium	SSL communication with high and medium encryption algorithms.		
	high	SSL communication with high encryption algorithms.		
	low	SSL communication with low encryption algorithms.		
	disable	Disable SSL communication.		
facility	Remote syslog facility.	option	-	local7
	<div><div>Option</div><div>Description</div></div>			
	kernel	Kernel messages.		

Parameter	Description	Type	Size	Default																																																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>user</i></td><td>Random user-level messages.</td></tr><tr><td><i>mail</i></td><td>Mail system.</td></tr><tr><td><i>daemon</i></td><td>System daemons.</td></tr><tr><td><i>auth</i></td><td>Security/authorization messages.</td></tr><tr><td><i>syslog</i></td><td>Messages generated internally by syslog.</td></tr><tr><td><i>lpr</i></td><td>Line printer subsystem.</td></tr><tr><td><i>news</i></td><td>Network news subsystem.</td></tr><tr><td><i>uucp</i></td><td>Network news subsystem.</td></tr><tr><td><i>cron</i></td><td>Clock daemon.</td></tr><tr><td><i>authpriv</i></td><td>Security/authorization messages (private).</td></tr><tr><td><i>ftp</i></td><td>FTP daemon.</td></tr><tr><td><i>ntp</i></td><td>NTP daemon.</td></tr><tr><td><i>audit</i></td><td>Log audit.</td></tr><tr><td><i>alert</i></td><td>Log alert.</td></tr><tr><td><i>clock</i></td><td>Clock daemon.</td></tr><tr><td><i>local0</i></td><td>Reserved for local use.</td></tr><tr><td><i>local1</i></td><td>Reserved for local use.</td></tr><tr><td><i>local2</i></td><td>Reserved for local use.</td></tr><tr><td><i>local3</i></td><td>Reserved for local use.</td></tr><tr><td><i>local4</i></td><td>Reserved for local use.</td></tr><tr><td><i>local5</i></td><td>Reserved for local use.</td></tr><tr><td><i>local6</i></td><td>Reserved for local use.</td></tr><tr><td><i>local7</i></td><td>Reserved for local use.</td></tr></table>	Option	Description	<i>user</i>	Random user-level messages.	<i>mail</i>	Mail system.	<i>daemon</i>	System daemons.	<i>auth</i>	Security/authorization messages.	<i>syslog</i>	Messages generated internally by syslog.	<i>lpr</i>	Line printer subsystem.	<i>news</i>	Network news subsystem.	<i>uucp</i>	Network news subsystem.	<i>cron</i>	Clock daemon.	<i>authpriv</i>	Security/authorization messages (private).	<i>ftp</i>	FTP daemon.	<i>ntp</i>	NTP daemon.	<i>audit</i>	Log audit.	<i>alert</i>	Log alert.	<i>clock</i>	Clock daemon.	<i>local0</i>	Reserved for local use.	<i>local1</i>	Reserved for local use.	<i>local2</i>	Reserved for local use.	<i>local3</i>	Reserved for local use.	<i>local4</i>	Reserved for local use.	<i>local5</i>	Reserved for local use.	<i>local6</i>	Reserved for local use.	<i>local7</i>	Reserved for local use.			
	Option	Description																																																		
	<i>user</i>	Random user-level messages.																																																		
	<i>mail</i>	Mail system.																																																		
	<i>daemon</i>	System daemons.																																																		
	<i>auth</i>	Security/authorization messages.																																																		
	<i>syslog</i>	Messages generated internally by syslog.																																																		
	<i>lpr</i>	Line printer subsystem.																																																		
	<i>news</i>	Network news subsystem.																																																		
	<i>uucp</i>	Network news subsystem.																																																		
	<i>cron</i>	Clock daemon.																																																		
	<i>authpriv</i>	Security/authorization messages (private).																																																		
	<i>ftp</i>	FTP daemon.																																																		
	<i>ntp</i>	NTP daemon.																																																		
	<i>audit</i>	Log audit.																																																		
	<i>alert</i>	Log alert.																																																		
	<i>clock</i>	Clock daemon.																																																		
	<i>local0</i>	Reserved for local use.																																																		
	<i>local1</i>	Reserved for local use.																																																		
	<i>local2</i>	Reserved for local use.																																																		
	<i>local3</i>	Reserved for local use.																																																		
	<i>local4</i>	Reserved for local use.																																																		
	<i>local5</i>	Reserved for local use.																																																		
<i>local6</i>	Reserved for local use.																																																			
<i>local7</i>	Reserved for local use.																																																			
format	Log format.	option	-	default																																																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>Syslog format.</td></tr><tr><td><i>csv</i></td><td>CSV (Comma Separated Values) format.</td></tr><tr><td><i>cef</i></td><td>CEF (Common Event Format) format.</td></tr><tr><td><i>rfc5424</i></td><td>Syslog RFC5424 format.</td></tr></table>	Option	Description	<i>default</i>	Syslog format.	<i>csv</i>	CSV (Comma Separated Values) format.	<i>cef</i>	CEF (Common Event Format) format.	<i>rfc5424</i>	Syslog RFC5424 format.																																									
	Option	Description																																																		
	<i>default</i>	Syslog format.																																																		
	<i>csv</i>	CSV (Comma Separated Values) format.																																																		
	<i>cef</i>	CEF (Common Event Format) format.																																																		
<i>rfc5424</i>	Syslog RFC5424 format.																																																			

Parameter	Description	Type	Size	Default								
interface	Specify outgoing interface to reach server.	string	Maximum length: 15									
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>auto</td><td>Set outgoing interface automatically.</td></tr><tr><td>sdwan</td><td>Set outgoing interface by SD-WAN or policy routing rules.</td></tr><tr><td>specify</td><td>Set outgoing interface manually.</td></tr></table>	Option	Description	auto	Set outgoing interface automatically.	sdwan	Set outgoing interface by SD-WAN or policy routing rules.	specify	Set outgoing interface manually.			
Option	Description											
auto	Set outgoing interface automatically.											
sdwan	Set outgoing interface by SD-WAN or policy routing rules.											
specify	Set outgoing interface manually.											
max-log-rate	Syslog maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0								
mode	Remote syslog logging over UDP/Reliable TCP.	option	-	udp								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>udp</td><td>Enable syslogging over UDP.</td></tr><tr><td>legacy-reliable</td><td>Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).</td></tr><tr><td>reliable</td><td>Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).</td></tr></table>	Option	Description	udp	Enable syslogging over UDP.	legacy-reliable	Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).	reliable	Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).			
Option	Description											
udp	Enable syslogging over UDP.											
legacy-reliable	Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).											
reliable	Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).											
port	Server listen port.	integer	Minimum value: 0 Maximum value: 65535	514								
priority	Set log transmission priority.	option	-	default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>default</td><td>Set Syslog transmission priority to default.</td></tr><tr><td>low</td><td>Set Syslog transmission priority to low.</td></tr></table>	Option	Description	default	Set Syslog transmission priority to default.	low	Set Syslog transmission priority to low.					
Option	Description											
default	Set Syslog transmission priority to default.											
low	Set Syslog transmission priority to low.											
server	Address of remote syslog server.	string	Maximum length: 127									
source-ip	Source IP address of syslog.	string	Maximum length: 63									
ssl-min-protocol-version	Minimum supported protocol version for SSL/TLS connections.	option	-	default								

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>default</i>	Follow system global setting.		
	<i>SSLv3</i>	SSLv3.		
	<i>TLSv1</i>	TLSv1.		
	<i>TLSv1-1</i>	TLSv1.1.		
	<i>TLSv1-2</i>	TLSv1.2.		
status	Enable/disable remote syslog logging.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Log to remote syslog server.		
	<i>disable</i>	Do not log to remote syslog server.		

### config custom-field-name

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 255	0
name	Field name.	string	Maximum length: 35	
custom	Field custom name.	string	Maximum length: 35	

### config log syslogd2 setting

Global settings for remote syslog server.

```

config log syslogd2 setting
    Description: Global settings for remote syslog server.
    set certificate {string}
    config custom-field-name
        Description: Custom field name for CEF format logging.
        edit <id>
            set name {string}
            set custom {string}
        next
    end
    set enc-algorithm [high-medium|high|...]
    set facility [kernel|user|...]
    set format [default|csv|...]

```

```

set interface {string}
set interface-select-method [auto|sdwan|...]
set max-log-rate {integer}
set mode [udp|legacy-reliable|...]
set port {integer}
set priority [default|low]
set server {string}
set source-ip {string}
set ssl-min-proto-version [default|SSLv3|...]
set status [enable|disable]
end

```

end

## config log syslogd2 setting

Parameter	Description	Type	Size	Default
certificate	Certificate used to communicate with Syslog server.	string	Maximum length: 35	
enc-algorithm	Enable/disable reliable syslogging with TLS encryption.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>high-medium</i>	SSL communication with high and medium encryption algorithms.		
	<i>high</i>	SSL communication with high encryption algorithms.		
	<i>low</i>	SSL communication with low encryption algorithms.		
	<i>disable</i>	Disable SSL communication.		
facility	Remote syslog facility.	option	-	local7
	<b>Option</b>	<b>Description</b>		
	<i>kernel</i>	Kernel messages.		
	<i>user</i>	Random user-level messages.		
	<i>mail</i>	Mail system.		
	<i>daemon</i>	System daemons.		
	<i>auth</i>	Security/authorization messages.		
	<i>syslog</i>	Messages generated internally by syslog.		
	<i>lpr</i>	Line printer subsystem.		
	<i>news</i>	Network news subsystem.		
	<i>uucp</i>	Network news subsystem.		
	<i>cron</i>	Clock daemon.		
	<i>authpriv</i>	Security/authorization messages (private).		
	<i>ftp</i>	FTP daemon.		



Parameter	Description	Type	Size	Default																										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ntp</i></td><td>NTP daemon.</td></tr><tr><td><i>audit</i></td><td>Log audit.</td></tr><tr><td><i>alert</i></td><td>Log alert.</td></tr><tr><td><i>clock</i></td><td>Clock daemon.</td></tr><tr><td><i>local0</i></td><td>Reserved for local use.</td></tr><tr><td><i>local1</i></td><td>Reserved for local use.</td></tr><tr><td><i>local2</i></td><td>Reserved for local use.</td></tr><tr><td><i>local3</i></td><td>Reserved for local use.</td></tr><tr><td><i>local4</i></td><td>Reserved for local use.</td></tr><tr><td><i>local5</i></td><td>Reserved for local use.</td></tr><tr><td><i>local6</i></td><td>Reserved for local use.</td></tr><tr><td><i>local7</i></td><td>Reserved for local use.</td></tr></table>	Option	Description	<i>ntp</i>	NTP daemon.	<i>audit</i>	Log audit.	<i>alert</i>	Log alert.	<i>clock</i>	Clock daemon.	<i>local0</i>	Reserved for local use.	<i>local1</i>	Reserved for local use.	<i>local2</i>	Reserved for local use.	<i>local3</i>	Reserved for local use.	<i>local4</i>	Reserved for local use.	<i>local5</i>	Reserved for local use.	<i>local6</i>	Reserved for local use.	<i>local7</i>	Reserved for local use.			
	Option	Description																												
	<i>ntp</i>	NTP daemon.																												
	<i>audit</i>	Log audit.																												
	<i>alert</i>	Log alert.																												
	<i>clock</i>	Clock daemon.																												
	<i>local0</i>	Reserved for local use.																												
	<i>local1</i>	Reserved for local use.																												
	<i>local2</i>	Reserved for local use.																												
	<i>local3</i>	Reserved for local use.																												
	<i>local4</i>	Reserved for local use.																												
	<i>local5</i>	Reserved for local use.																												
	<i>local6</i>	Reserved for local use.																												
<i>local7</i>	Reserved for local use.																													
format	Log format.	option	-	default																										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>Syslog format.</td></tr><tr><td><i>csv</i></td><td>CSV (Comma Separated Values) format.</td></tr><tr><td><i>cef</i></td><td>CEF (Common Event Format) format.</td></tr><tr><td><i>rfc5424</i></td><td>Syslog RFC5424 format.</td></tr></table>	Option	Description	<i>default</i>	Syslog format.	<i>csv</i>	CSV (Comma Separated Values) format.	<i>cef</i>	CEF (Common Event Format) format.	<i>rfc5424</i>	Syslog RFC5424 format.																			
	Option	Description																												
	<i>default</i>	Syslog format.																												
	<i>csv</i>	CSV (Comma Separated Values) format.																												
	<i>cef</i>	CEF (Common Event Format) format.																												
<i>rfc5424</i>	Syslog RFC5424 format.																													
interface	Specify outgoing interface to reach server.	string	Maximum length: 15																											
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto																										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto</i></td><td>Set outgoing interface automatically.</td></tr><tr><td><i>sdwan</i></td><td>Set outgoing interface by SD-WAN or policy routing rules.</td></tr><tr><td><i>specify</i></td><td>Set outgoing interface manually.</td></tr></table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.																					
	Option	Description																												
	<i>auto</i>	Set outgoing interface automatically.																												
	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.																												
<i>specify</i>	Set outgoing interface manually.																													

Parameter	Description	Type	Size	Default												
max-log-rate	Syslog maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0												
mode	Remote syslog logging over UDP/Reliable TCP.	option	-	udp												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>udp</td><td>Enable syslogging over UDP.</td></tr><tr><td>legacy-reliable</td><td>Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).</td></tr><tr><td>reliable</td><td>Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).</td></tr></table>	Option	Description	udp	Enable syslogging over UDP.	legacy-reliable	Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).	reliable	Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).							
	Option	Description														
	udp	Enable syslogging over UDP.														
	legacy-reliable	Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).														
reliable	Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).															
port	Server listen port.	integer	Minimum value: 0 Maximum value: 65535	514												
priority	Set log transmission priority.	option	-	default												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>default</td><td>Set Syslog transmission priority to default.</td></tr><tr><td>low</td><td>Set Syslog transmission priority to low.</td></tr></table>	Option	Description	default	Set Syslog transmission priority to default.	low	Set Syslog transmission priority to low.									
	Option	Description														
	default	Set Syslog transmission priority to default.														
low	Set Syslog transmission priority to low.															
server	Address of remote syslog server.	string	Maximum length: 127													
source-ip	Source IP address of syslog.	string	Maximum length: 63													
ssl-min-protocol-version	Minimum supported protocol version for SSL/TLS connections.	option	-	default												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>default</td><td>Follow system global setting.</td></tr><tr><td>SSLv3</td><td>SSLv3.</td></tr><tr><td>TLSv1</td><td>TLSv1.</td></tr><tr><td>TLSv1-1</td><td>TLSv1.1.</td></tr><tr><td>TLSv1-2</td><td>TLSv1.2.</td></tr></table>	Option	Description	default	Follow system global setting.	SSLv3	SSLv3.	TLSv1	TLSv1.	TLSv1-1	TLSv1.1.	TLSv1-2	TLSv1.2.			
	Option	Description														
	default	Follow system global setting.														
	SSLv3	SSLv3.														
	TLSv1	TLSv1.														
	TLSv1-1	TLSv1.1.														
TLSv1-2	TLSv1.2.															
status	Enable/disable remote syslog logging.	option	-	disable												

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Log to remote syslog server.		
	<i>disable</i>	Do not log to remote syslog server.		

### config custom-field-name

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 255	0
name	Field name.	string	Maximum length: 35	
custom	Field custom name.	string	Maximum length: 35	

### config log syslogd3 filter

Filters for remote system server.

```
config log syslogd3 filter
    Description: Filters for remote system server.
    set anomaly [enable|disable]
    set forward-traffic [enable|disable]
    config free-style
        Description: Free style filters.
        edit <id>
            set category [traffic|event|...]
            set filter {string}
            set filter-type [include|exclude]
        next
    end
    set gtp [enable|disable]
    set local-traffic [enable|disable]
    set multicast-traffic [enable|disable]
    set severity [emergency|alert|...]
    set sniffer-traffic [enable|disable]
    set voip [enable|disable]
    set ztna-traffic [enable|disable]
end
```

## config log syslogd3 filter

Parameter	Description	Type	Size	Default										
anomaly	Enable/disable anomaly logging.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable anomaly logging.</td></tr><tr><td><i>disable</i></td><td>Disable anomaly logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable anomaly logging.	<i>disable</i>	Disable anomaly logging.							
Option	Description													
<i>enable</i>	Enable anomaly logging.													
<i>disable</i>	Disable anomaly logging.													
forward-traffic	Enable/disable forward traffic logging.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable forward traffic logging.</td></tr><tr><td><i>disable</i></td><td>Disable forward traffic logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable forward traffic logging.	<i>disable</i>	Disable forward traffic logging.							
Option	Description													
<i>enable</i>	Enable forward traffic logging.													
<i>disable</i>	Disable forward traffic logging.													
gtp *	Enable/disable GTP messages logging.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable GTP messages logging.</td></tr><tr><td><i>disable</i></td><td>Disable GTP messages logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable GTP messages logging.	<i>disable</i>	Disable GTP messages logging.							
Option	Description													
<i>enable</i>	Enable GTP messages logging.													
<i>disable</i>	Disable GTP messages logging.													
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable local in or out traffic logging.</td></tr><tr><td><i>disable</i></td><td>Disable local in or out traffic logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable local in or out traffic logging.	<i>disable</i>	Disable local in or out traffic logging.							
Option	Description													
<i>enable</i>	Enable local in or out traffic logging.													
<i>disable</i>	Disable local in or out traffic logging.													
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable multicast traffic logging.</td></tr><tr><td><i>disable</i></td><td>Disable multicast traffic logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable multicast traffic logging.	<i>disable</i>	Disable multicast traffic logging.							
Option	Description													
<i>enable</i>	Enable multicast traffic logging.													
<i>disable</i>	Disable multicast traffic logging.													
severity	Lowest severity level to log.	option	-	information										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>emergency</i></td><td>Emergency level.</td></tr><tr><td><i>alert</i></td><td>Alert level.</td></tr><tr><td><i>critical</i></td><td>Critical level.</td></tr><tr><td><i>error</i></td><td>Error level.</td></tr></table>	Option	Description	<i>emergency</i>	Emergency level.	<i>alert</i>	Alert level.	<i>critical</i>	Critical level.	<i>error</i>	Error level.			
Option	Description													
<i>emergency</i>	Emergency level.													
<i>alert</i>	Alert level.													
<i>critical</i>	Critical level.													
<i>error</i>	Error level.													

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>warning</i>	Warning level.		
	<i>notification</i>	Notification level.		
	<i>information</i>	Information level.		
	<i>debug</i>	Debug level.		
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable sniffer traffic logging.		
	<i>disable</i>	Disable sniffer traffic logging.		
voip	Enable/disable VoIP logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable VoIP logging.		
	<i>disable</i>	Disable VoIP logging.		
ztna-traffic	Enable/disable ztna traffic logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable ztna traffic logging.		
	<i>disable</i>	Disable ztna traffic logging.		

\* This parameter may not exist in some models.

### config free-style

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
category	Log category.	option	-	traffic
	<b>Option</b>	<b>Description</b>		
	<i>traffic</i>	Traffic log.		

Parameter	Description	Type	Size	Default																																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>event</i></td><td>Event log.</td></tr><tr><td><i>virus</i></td><td>Antivirus log.</td></tr><tr><td><i>webfilter</i></td><td>Web filter log.</td></tr><tr><td><i>attack</i></td><td>Attack log.</td></tr><tr><td><i>spam</i></td><td>Antispam log.</td></tr><tr><td><i>anomaly</i></td><td>Anomaly log.</td></tr><tr><td><i>voip</i></td><td>VoIP log.</td></tr><tr><td><i>dlp</i></td><td>DLP log.</td></tr><tr><td><i>app-ctrl</i></td><td>Application control log.</td></tr><tr><td><i>waf</i></td><td>Web application firewall log.</td></tr><tr><td><i>dns</i></td><td>DNS detail log.</td></tr><tr><td><i>ssh</i></td><td>SSH log.</td></tr><tr><td><i>ssl</i></td><td>SSL log.</td></tr><tr><td><i>file-filter</i></td><td>File filter log.</td></tr><tr><td><i>icap</i></td><td>ICAP log.</td></tr></table>	Option	Description	<i>event</i>	Event log.	<i>virus</i>	Antivirus log.	<i>webfilter</i>	Web filter log.	<i>attack</i>	Attack log.	<i>spam</i>	Antispam log.	<i>anomaly</i>	Anomaly log.	<i>voip</i>	VoIP log.	<i>dlp</i>	DLP log.	<i>app-ctrl</i>	Application control log.	<i>waf</i>	Web application firewall log.	<i>dns</i>	DNS detail log.	<i>ssh</i>	SSH log.	<i>ssl</i>	SSL log.	<i>file-filter</i>	File filter log.	<i>icap</i>	ICAP log.			
	Option	Description																																		
	<i>event</i>	Event log.																																		
	<i>virus</i>	Antivirus log.																																		
	<i>webfilter</i>	Web filter log.																																		
	<i>attack</i>	Attack log.																																		
	<i>spam</i>	Antispam log.																																		
	<i>anomaly</i>	Anomaly log.																																		
	<i>voip</i>	VoIP log.																																		
	<i>dlp</i>	DLP log.																																		
	<i>app-ctrl</i>	Application control log.																																		
	<i>waf</i>	Web application firewall log.																																		
	<i>dns</i>	DNS detail log.																																		
	<i>ssh</i>	SSH log.																																		
	<i>ssl</i>	SSL log.																																		
	<i>file-filter</i>	File filter log.																																		
<i>icap</i>	ICAP log.																																			
filter	Free style filter string.	string	Maximum length: 1023																																	
filter-type	Include/exclude logs that match the filter.	option	-	include																																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>include</i></td><td>Include logs that match the filter.</td></tr><tr><td><i>exclude</i></td><td>Exclude logs that match the filter.</td></tr></table>	Option	Description	<i>include</i>	Include logs that match the filter.	<i>exclude</i>	Exclude logs that match the filter.																													
	Option	Description																																		
	<i>include</i>	Include logs that match the filter.																																		
<i>exclude</i>	Exclude logs that match the filter.																																			

## config log syslogd3 override-filter

Override filters for remote system server.

```

config log syslogd3 override-filter
    Description: Override filters for remote system server.
    set anomaly [enable|disable]
    set forward-traffic [enable|disable]
    config free-style
        Description: Free style filters.
        edit <id>
            set category [traffic|event|...]
            set filter {string}

```

```

        set filter-type [include|exclude]
    next
end
set gtp [enable|disable]
set local-traffic [enable|disable]
set multicast-traffic [enable|disable]
set severity [emergency|alert|...]
set sniffer-traffic [enable|disable]
set voip [enable|disable]
set ztna-traffic [enable|disable]
end

```

## config log syslogd3 override-filter

Parameter	Description	Type	Size	Default						
anomaly	Enable/disable anomaly logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable anomaly logging.</td></tr><tr><td><i>disable</i></td><td>Disable anomaly logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable anomaly logging.	<i>disable</i>	Disable anomaly logging.			
Option	Description									
<i>enable</i>	Enable anomaly logging.									
<i>disable</i>	Disable anomaly logging.									
forward-traffic	Enable/disable forward traffic logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable forward traffic logging.</td></tr><tr><td><i>disable</i></td><td>Disable forward traffic logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable forward traffic logging.	<i>disable</i>	Disable forward traffic logging.			
Option	Description									
<i>enable</i>	Enable forward traffic logging.									
<i>disable</i>	Disable forward traffic logging.									
gtp *	Enable/disable GTP messages logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable GTP messages logging.</td></tr><tr><td><i>disable</i></td><td>Disable GTP messages logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable GTP messages logging.	<i>disable</i>	Disable GTP messages logging.			
Option	Description									
<i>enable</i>	Enable GTP messages logging.									
<i>disable</i>	Disable GTP messages logging.									
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable local in or out traffic logging.</td></tr><tr><td><i>disable</i></td><td>Disable local in or out traffic logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable local in or out traffic logging.	<i>disable</i>	Disable local in or out traffic logging.			
Option	Description									
<i>enable</i>	Enable local in or out traffic logging.									
<i>disable</i>	Disable local in or out traffic logging.									
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable multicast traffic logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable multicast traffic logging.					
Option	Description									
<i>enable</i>	Enable multicast traffic logging.									

Parameter	Description	Type	Size	Default																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable multicast traffic logging.</td></tr></table>	Option	Description	<i>disable</i>	Disable multicast traffic logging.																	
	Option	Description																				
<i>disable</i>	Disable multicast traffic logging.																					
severity	Lowest severity level to log.	option	-	information																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>emergency</i></td><td>Emergency level.</td></tr><tr><td><i>alert</i></td><td>Alert level.</td></tr><tr><td><i>critical</i></td><td>Critical level.</td></tr><tr><td><i>error</i></td><td>Error level.</td></tr><tr><td><i>warning</i></td><td>Warning level.</td></tr><tr><td><i>notification</i></td><td>Notification level.</td></tr><tr><td><i>information</i></td><td>Information level.</td></tr><tr><td><i>debug</i></td><td>Debug level.</td></tr></table>	Option	Description	<i>emergency</i>	Emergency level.	<i>alert</i>	Alert level.	<i>critical</i>	Critical level.	<i>error</i>	Error level.	<i>warning</i>	Warning level.	<i>notification</i>	Notification level.	<i>information</i>	Information level.	<i>debug</i>	Debug level.			
	Option	Description																				
	<i>emergency</i>	Emergency level.																				
	<i>alert</i>	Alert level.																				
	<i>critical</i>	Critical level.																				
	<i>error</i>	Error level.																				
	<i>warning</i>	Warning level.																				
	<i>notification</i>	Notification level.																				
	<i>information</i>	Information level.																				
<i>debug</i>	Debug level.																					
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable sniffer traffic logging.</td></tr><tr><td><i>disable</i></td><td>Disable sniffer traffic logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable sniffer traffic logging.	<i>disable</i>	Disable sniffer traffic logging.															
	Option	Description																				
	<i>enable</i>	Enable sniffer traffic logging.																				
<i>disable</i>	Disable sniffer traffic logging.																					
voip	Enable/disable VoIP logging.	option	-	enable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable VoIP logging.</td></tr><tr><td><i>disable</i></td><td>Disable VoIP logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable VoIP logging.	<i>disable</i>	Disable VoIP logging.															
	Option	Description																				
	<i>enable</i>	Enable VoIP logging.																				
<i>disable</i>	Disable VoIP logging.																					
ztna-traffic	Enable/disable ztna traffic logging.	option	-	enable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable ztna traffic logging.</td></tr><tr><td><i>disable</i></td><td>Disable ztna traffic logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable ztna traffic logging.	<i>disable</i>	Disable ztna traffic logging.															
	Option	Description																				
	<i>enable</i>	Enable ztna traffic logging.																				
<i>disable</i>	Disable ztna traffic logging.																					

\* This parameter may not exist in some models.



## config free-style

Parameter	Description	Type	Size	Default																																		
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0																																		
category	Log category.	option	-	traffic																																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>traffic</td><td>Traffic log.</td></tr><tr><td>event</td><td>Event log.</td></tr><tr><td>virus</td><td>Antivirus log.</td></tr><tr><td>webfilter</td><td>Web filter log.</td></tr><tr><td>attack</td><td>Attack log.</td></tr><tr><td>spam</td><td>Antispam log.</td></tr><tr><td>anomaly</td><td>Anomaly log.</td></tr><tr><td>voip</td><td>VoIP log.</td></tr><tr><td>dlp</td><td>DLP log.</td></tr><tr><td>app-ctrl</td><td>Application control log.</td></tr><tr><td>waf</td><td>Web application firewall log.</td></tr><tr><td>dns</td><td>DNS detail log.</td></tr><tr><td>ssh</td><td>SSH log.</td></tr><tr><td>ssl</td><td>SSL log.</td></tr><tr><td>file-filter</td><td>File filter log.</td></tr><tr><td>icap</td><td>ICAP log.</td></tr></table>	Option	Description	traffic	Traffic log.	event	Event log.	virus	Antivirus log.	webfilter	Web filter log.	attack	Attack log.	spam	Antispam log.	anomaly	Anomaly log.	voip	VoIP log.	dlp	DLP log.	app-ctrl	Application control log.	waf	Web application firewall log.	dns	DNS detail log.	ssh	SSH log.	ssl	SSL log.	file-filter	File filter log.	icap	ICAP log.			
	Option	Description																																				
	traffic	Traffic log.																																				
	event	Event log.																																				
	virus	Antivirus log.																																				
	webfilter	Web filter log.																																				
	attack	Attack log.																																				
	spam	Antispam log.																																				
	anomaly	Anomaly log.																																				
	voip	VoIP log.																																				
	dlp	DLP log.																																				
	app-ctrl	Application control log.																																				
	waf	Web application firewall log.																																				
	dns	DNS detail log.																																				
	ssh	SSH log.																																				
	ssl	SSL log.																																				
	file-filter	File filter log.																																				
icap	ICAP log.																																					
filter	Free style filter string.	string	Maximum length: 1023																																			
filter-type	Include/exclude logs that match the filter.	option	-	include																																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>include</td><td>Include logs that match the filter.</td></tr><tr><td>exclude</td><td>Exclude logs that match the filter.</td></tr></table>	Option	Description	include	Include logs that match the filter.	exclude	Exclude logs that match the filter.																															
	Option	Description																																				
	include	Include logs that match the filter.																																				
exclude	Exclude logs that match the filter.																																					

## config log syslogd3 override-setting

Override settings for remote syslog server.

```
config log syslogd3 override-setting
  Description: Override settings for remote syslog server.
  set certificate {string}
  config custom-field-name
    Description: Custom field name for CEF format logging.
    edit <id>
      set name {string}
      set custom {string}
    next
  end
  set enc-algorithm [high-medium|high|...]
  set facility [kernel|user|...]
  set format [default|csv|...]
  set interface {string}
  set interface-select-method [auto|sdwan|...]
  set max-log-rate {integer}
  set mode [udp|legacy-reliable|...]
  set port {integer}
  set priority [default|low]
  set server {string}
  set source-ip {string}
  set ssl-min-proto-version [default|SSLv3|...]
  set status [enable|disable]
end
```

## config log syslogd3 override-setting

Parameter	Description	Type	Size	Default
certificate	Certificate used to communicate with Syslog server.	string	Maximum length: 35	
enc-algorithm	Enable/disable reliable syslogging with TLS encryption.	option	-	disable
	<div><div>Option</div><div>Description</div></div>			
	high-medium	SSL communication with high and medium encryption algorithms.		
	high	SSL communication with high encryption algorithms.		
	low	SSL communication with low encryption algorithms.		
	disable	Disable SSL communication.		
facility	Remote syslog facility.	option	-	local7
	<div><div>Option</div><div>Description</div></div>			
	kernel	Kernel messages.		

Parameter	Description	Type	Size	Default																																																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>user</i></td><td>Random user-level messages.</td></tr><tr><td><i>mail</i></td><td>Mail system.</td></tr><tr><td><i>daemon</i></td><td>System daemons.</td></tr><tr><td><i>auth</i></td><td>Security/authorization messages.</td></tr><tr><td><i>syslog</i></td><td>Messages generated internally by syslog.</td></tr><tr><td><i>lpr</i></td><td>Line printer subsystem.</td></tr><tr><td><i>news</i></td><td>Network news subsystem.</td></tr><tr><td><i>uucp</i></td><td>Network news subsystem.</td></tr><tr><td><i>cron</i></td><td>Clock daemon.</td></tr><tr><td><i>authpriv</i></td><td>Security/authorization messages (private).</td></tr><tr><td><i>ftp</i></td><td>FTP daemon.</td></tr><tr><td><i>ntp</i></td><td>NTP daemon.</td></tr><tr><td><i>audit</i></td><td>Log audit.</td></tr><tr><td><i>alert</i></td><td>Log alert.</td></tr><tr><td><i>clock</i></td><td>Clock daemon.</td></tr><tr><td><i>local0</i></td><td>Reserved for local use.</td></tr><tr><td><i>local1</i></td><td>Reserved for local use.</td></tr><tr><td><i>local2</i></td><td>Reserved for local use.</td></tr><tr><td><i>local3</i></td><td>Reserved for local use.</td></tr><tr><td><i>local4</i></td><td>Reserved for local use.</td></tr><tr><td><i>local5</i></td><td>Reserved for local use.</td></tr><tr><td><i>local6</i></td><td>Reserved for local use.</td></tr><tr><td><i>local7</i></td><td>Reserved for local use.</td></tr></table>	Option	Description	<i>user</i>	Random user-level messages.	<i>mail</i>	Mail system.	<i>daemon</i>	System daemons.	<i>auth</i>	Security/authorization messages.	<i>syslog</i>	Messages generated internally by syslog.	<i>lpr</i>	Line printer subsystem.	<i>news</i>	Network news subsystem.	<i>uucp</i>	Network news subsystem.	<i>cron</i>	Clock daemon.	<i>authpriv</i>	Security/authorization messages (private).	<i>ftp</i>	FTP daemon.	<i>ntp</i>	NTP daemon.	<i>audit</i>	Log audit.	<i>alert</i>	Log alert.	<i>clock</i>	Clock daemon.	<i>local0</i>	Reserved for local use.	<i>local1</i>	Reserved for local use.	<i>local2</i>	Reserved for local use.	<i>local3</i>	Reserved for local use.	<i>local4</i>	Reserved for local use.	<i>local5</i>	Reserved for local use.	<i>local6</i>	Reserved for local use.	<i>local7</i>	Reserved for local use.			
	Option	Description																																																		
	<i>user</i>	Random user-level messages.																																																		
	<i>mail</i>	Mail system.																																																		
	<i>daemon</i>	System daemons.																																																		
	<i>auth</i>	Security/authorization messages.																																																		
	<i>syslog</i>	Messages generated internally by syslog.																																																		
	<i>lpr</i>	Line printer subsystem.																																																		
	<i>news</i>	Network news subsystem.																																																		
	<i>uucp</i>	Network news subsystem.																																																		
	<i>cron</i>	Clock daemon.																																																		
	<i>authpriv</i>	Security/authorization messages (private).																																																		
	<i>ftp</i>	FTP daemon.																																																		
	<i>ntp</i>	NTP daemon.																																																		
	<i>audit</i>	Log audit.																																																		
	<i>alert</i>	Log alert.																																																		
	<i>clock</i>	Clock daemon.																																																		
	<i>local0</i>	Reserved for local use.																																																		
	<i>local1</i>	Reserved for local use.																																																		
	<i>local2</i>	Reserved for local use.																																																		
	<i>local3</i>	Reserved for local use.																																																		
	<i>local4</i>	Reserved for local use.																																																		
	<i>local5</i>	Reserved for local use.																																																		
<i>local6</i>	Reserved for local use.																																																			
<i>local7</i>	Reserved for local use.																																																			
format	Log format.	option	-	default																																																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>Syslog format.</td></tr><tr><td><i>csv</i></td><td>CSV (Comma Separated Values) format.</td></tr><tr><td><i>cef</i></td><td>CEF (Common Event Format) format.</td></tr><tr><td><i>rfc5424</i></td><td>Syslog RFC5424 format.</td></tr></table>	Option	Description	<i>default</i>	Syslog format.	<i>csv</i>	CSV (Comma Separated Values) format.	<i>cef</i>	CEF (Common Event Format) format.	<i>rfc5424</i>	Syslog RFC5424 format.																																									
	Option	Description																																																		
	<i>default</i>	Syslog format.																																																		
	<i>csv</i>	CSV (Comma Separated Values) format.																																																		
	<i>cef</i>	CEF (Common Event Format) format.																																																		
<i>rfc5424</i>	Syslog RFC5424 format.																																																			

Parameter	Description	Type	Size	Default								
interface	Specify outgoing interface to reach server.	string	Maximum length: 15									
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>auto</td><td>Set outgoing interface automatically.</td></tr><tr><td>sdwan</td><td>Set outgoing interface by SD-WAN or policy routing rules.</td></tr><tr><td>specify</td><td>Set outgoing interface manually.</td></tr></table>	Option	Description	auto	Set outgoing interface automatically.	sdwan	Set outgoing interface by SD-WAN or policy routing rules.	specify	Set outgoing interface manually.			
Option	Description											
auto	Set outgoing interface automatically.											
sdwan	Set outgoing interface by SD-WAN or policy routing rules.											
specify	Set outgoing interface manually.											
max-log-rate	Syslog maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0								
mode	Remote syslog logging over UDP/Reliable TCP.	option	-	udp								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>udp</td><td>Enable syslogging over UDP.</td></tr><tr><td>legacy-reliable</td><td>Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).</td></tr><tr><td>reliable</td><td>Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).</td></tr></table>	Option	Description	udp	Enable syslogging over UDP.	legacy-reliable	Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).	reliable	Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).			
Option	Description											
udp	Enable syslogging over UDP.											
legacy-reliable	Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).											
reliable	Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).											
port	Server listen port.	integer	Minimum value: 0 Maximum value: 65535	514								
priority	Set log transmission priority.	option	-	default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>default</td><td>Set Syslog transmission priority to default.</td></tr><tr><td>low</td><td>Set Syslog transmission priority to low.</td></tr></table>	Option	Description	default	Set Syslog transmission priority to default.	low	Set Syslog transmission priority to low.					
Option	Description											
default	Set Syslog transmission priority to default.											
low	Set Syslog transmission priority to low.											
server	Address of remote syslog server.	string	Maximum length: 127									
source-ip	Source IP address of syslog.	string	Maximum length: 63									
ssl-min-protocol-version	Minimum supported protocol version for SSL/TLS connections.	option	-	default								

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>default</i>	Follow system global setting.		
	<i>SSLv3</i>	SSLv3.		
	<i>TLSv1</i>	TLSv1.		
	<i>TLSv1-1</i>	TLSv1.1.		
	<i>TLSv1-2</i>	TLSv1.2.		
status	Enable/disable remote syslog logging.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Log to remote syslog server.		
	<i>disable</i>	Do not log to remote syslog server.		

### config custom-field-name

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 255	0
name	Field name.	string	Maximum length: 35	
custom	Field custom name.	string	Maximum length: 35	

## config log syslogd3 setting

Global settings for remote syslog server.

```
config log syslogd3 setting
    Description: Global settings for remote syslog server.
    set certificate {string}
    config custom-field-name
        Description: Custom field name for CEF format logging.
        edit <id>
            set name {string}
            set custom {string}
        next
    end
    set enc-algorithm [high-medium|high|...]
    set facility [kernel|user|...]
    set format [default|csv|...]
```

```

set interface {string}
set interface-select-method [auto|sdwan|...]
set max-log-rate {integer}
set mode [udp|legacy-reliable|...]
set port {integer}
set priority [default|low]
set server {string}
set source-ip {string}
set ssl-min-proto-version [default|SSLv3|...]
set status [enable|disable]
end

```

end

## config log syslogd3 setting

Parameter	Description	Type	Size	Default
certificate	Certificate used to communicate with Syslog server.	string	Maximum length: 35	
enc-algorithm	Enable/disable reliable syslogging with TLS encryption.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>high-medium</i>	SSL communication with high and medium encryption algorithms.		
	<i>high</i>	SSL communication with high encryption algorithms.		
	<i>low</i>	SSL communication with low encryption algorithms.		
	<i>disable</i>	Disable SSL communication.		
facility	Remote syslog facility.	option	-	local7
	<b>Option</b>	<b>Description</b>		
	<i>kernel</i>	Kernel messages.		
	<i>user</i>	Random user-level messages.		
	<i>mail</i>	Mail system.		
	<i>daemon</i>	System daemons.		
	<i>auth</i>	Security/authorization messages.		
	<i>syslog</i>	Messages generated internally by syslog.		
	<i>lpr</i>	Line printer subsystem.		
	<i>news</i>	Network news subsystem.		
	<i>uucp</i>	Network news subsystem.		
	<i>cron</i>	Clock daemon.		
	<i>authpriv</i>	Security/authorization messages (private).		
	<i>ftp</i>	FTP daemon.		

Parameter	Description	Type	Size	Default																										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ntp</i></td><td>NTP daemon.</td></tr><tr><td><i>audit</i></td><td>Log audit.</td></tr><tr><td><i>alert</i></td><td>Log alert.</td></tr><tr><td><i>clock</i></td><td>Clock daemon.</td></tr><tr><td><i>local0</i></td><td>Reserved for local use.</td></tr><tr><td><i>local1</i></td><td>Reserved for local use.</td></tr><tr><td><i>local2</i></td><td>Reserved for local use.</td></tr><tr><td><i>local3</i></td><td>Reserved for local use.</td></tr><tr><td><i>local4</i></td><td>Reserved for local use.</td></tr><tr><td><i>local5</i></td><td>Reserved for local use.</td></tr><tr><td><i>local6</i></td><td>Reserved for local use.</td></tr><tr><td><i>local7</i></td><td>Reserved for local use.</td></tr></table>	Option	Description	<i>ntp</i>	NTP daemon.	<i>audit</i>	Log audit.	<i>alert</i>	Log alert.	<i>clock</i>	Clock daemon.	<i>local0</i>	Reserved for local use.	<i>local1</i>	Reserved for local use.	<i>local2</i>	Reserved for local use.	<i>local3</i>	Reserved for local use.	<i>local4</i>	Reserved for local use.	<i>local5</i>	Reserved for local use.	<i>local6</i>	Reserved for local use.	<i>local7</i>	Reserved for local use.			
	Option	Description																												
	<i>ntp</i>	NTP daemon.																												
	<i>audit</i>	Log audit.																												
	<i>alert</i>	Log alert.																												
	<i>clock</i>	Clock daemon.																												
	<i>local0</i>	Reserved for local use.																												
	<i>local1</i>	Reserved for local use.																												
	<i>local2</i>	Reserved for local use.																												
	<i>local3</i>	Reserved for local use.																												
	<i>local4</i>	Reserved for local use.																												
	<i>local5</i>	Reserved for local use.																												
	<i>local6</i>	Reserved for local use.																												
<i>local7</i>	Reserved for local use.																													
format	Log format.	option	-	default																										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>Syslog format.</td></tr><tr><td><i>csv</i></td><td>CSV (Comma Separated Values) format.</td></tr><tr><td><i>cef</i></td><td>CEF (Common Event Format) format.</td></tr><tr><td><i>rfc5424</i></td><td>Syslog RFC5424 format.</td></tr></table>	Option	Description	<i>default</i>	Syslog format.	<i>csv</i>	CSV (Comma Separated Values) format.	<i>cef</i>	CEF (Common Event Format) format.	<i>rfc5424</i>	Syslog RFC5424 format.																			
	Option	Description																												
	<i>default</i>	Syslog format.																												
	<i>csv</i>	CSV (Comma Separated Values) format.																												
	<i>cef</i>	CEF (Common Event Format) format.																												
<i>rfc5424</i>	Syslog RFC5424 format.																													
interface	Specify outgoing interface to reach server.	string	Maximum length: 15																											
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto																										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto</i></td><td>Set outgoing interface automatically.</td></tr><tr><td><i>sdwan</i></td><td>Set outgoing interface by SD-WAN or policy routing rules.</td></tr><tr><td><i>specify</i></td><td>Set outgoing interface manually.</td></tr></table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.																					
	Option	Description																												
	<i>auto</i>	Set outgoing interface automatically.																												
	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.																												
<i>specify</i>	Set outgoing interface manually.																													

Parameter	Description	Type	Size	Default												
max-log-rate	Syslog maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0												
mode	Remote syslog logging over UDP/Reliable TCP.	option	-	udp												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>udp</td><td>Enable syslogging over UDP.</td></tr><tr><td>legacy-reliable</td><td>Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).</td></tr><tr><td>reliable</td><td>Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).</td></tr></table>	Option	Description	udp	Enable syslogging over UDP.	legacy-reliable	Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).	reliable	Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).							
	Option	Description														
	udp	Enable syslogging over UDP.														
	legacy-reliable	Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).														
reliable	Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).															
port	Server listen port.	integer	Minimum value: 0 Maximum value: 65535	514												
priority	Set log transmission priority.	option	-	default												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>default</td><td>Set Syslog transmission priority to default.</td></tr><tr><td>low</td><td>Set Syslog transmission priority to low.</td></tr></table>	Option	Description	default	Set Syslog transmission priority to default.	low	Set Syslog transmission priority to low.									
	Option	Description														
	default	Set Syslog transmission priority to default.														
low	Set Syslog transmission priority to low.															
server	Address of remote syslog server.	string	Maximum length: 127													
source-ip	Source IP address of syslog.	string	Maximum length: 63													
ssl-min-protocol-version	Minimum supported protocol version for SSL/TLS connections.	option	-	default												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>default</td><td>Follow system global setting.</td></tr><tr><td>SSLv3</td><td>SSLv3.</td></tr><tr><td>TLSv1</td><td>TLSv1.</td></tr><tr><td>TLSv1-1</td><td>TLSv1.1.</td></tr><tr><td>TLSv1-2</td><td>TLSv1.2.</td></tr></table>	Option	Description	default	Follow system global setting.	SSLv3	SSLv3.	TLSv1	TLSv1.	TLSv1-1	TLSv1.1.	TLSv1-2	TLSv1.2.			
	Option	Description														
	default	Follow system global setting.														
	SSLv3	SSLv3.														
	TLSv1	TLSv1.														
	TLSv1-1	TLSv1.1.														
TLSv1-2	TLSv1.2.															
status	Enable/disable remote syslog logging.	option	-	disable												



Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Log to remote syslog server.		
	<i>disable</i>	Do not log to remote syslog server.		

### config custom-field-name

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 255	0
name	Field name.	string	Maximum length: 35	
custom	Field custom name.	string	Maximum length: 35	

### config log syslogd4 filter

Filters for remote system server.

```

config log syslogd4 filter
    Description: Filters for remote system server.
    set anomaly [enable|disable]
    set forward-traffic [enable|disable]
    config free-style
        Description: Free style filters.
        edit <id>
            set category [traffic|event|...]
            set filter {string}
            set filter-type [include|exclude]
        next
    end
    set gtp [enable|disable]
    set local-traffic [enable|disable]
    set multicast-traffic [enable|disable]
    set severity [emergency|alert|...]
    set sniffer-traffic [enable|disable]
    set voip [enable|disable]
    set ztna-traffic [enable|disable]
end

```

## config log syslogd4 filter

Parameter	Description	Type	Size	Default										
anomaly	Enable/disable anomaly logging.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable anomaly logging.</td></tr><tr><td><i>disable</i></td><td>Disable anomaly logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable anomaly logging.	<i>disable</i>	Disable anomaly logging.							
Option	Description													
<i>enable</i>	Enable anomaly logging.													
<i>disable</i>	Disable anomaly logging.													
forward-traffic	Enable/disable forward traffic logging.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable forward traffic logging.</td></tr><tr><td><i>disable</i></td><td>Disable forward traffic logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable forward traffic logging.	<i>disable</i>	Disable forward traffic logging.							
Option	Description													
<i>enable</i>	Enable forward traffic logging.													
<i>disable</i>	Disable forward traffic logging.													
gtp *	Enable/disable GTP messages logging.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable GTP messages logging.</td></tr><tr><td><i>disable</i></td><td>Disable GTP messages logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable GTP messages logging.	<i>disable</i>	Disable GTP messages logging.							
Option	Description													
<i>enable</i>	Enable GTP messages logging.													
<i>disable</i>	Disable GTP messages logging.													
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable local in or out traffic logging.</td></tr><tr><td><i>disable</i></td><td>Disable local in or out traffic logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable local in or out traffic logging.	<i>disable</i>	Disable local in or out traffic logging.							
Option	Description													
<i>enable</i>	Enable local in or out traffic logging.													
<i>disable</i>	Disable local in or out traffic logging.													
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable multicast traffic logging.</td></tr><tr><td><i>disable</i></td><td>Disable multicast traffic logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable multicast traffic logging.	<i>disable</i>	Disable multicast traffic logging.							
Option	Description													
<i>enable</i>	Enable multicast traffic logging.													
<i>disable</i>	Disable multicast traffic logging.													
severity	Lowest severity level to log.	option	-	information										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>emergency</i></td><td>Emergency level.</td></tr><tr><td><i>alert</i></td><td>Alert level.</td></tr><tr><td><i>critical</i></td><td>Critical level.</td></tr><tr><td><i>error</i></td><td>Error level.</td></tr></table>	Option	Description	<i>emergency</i>	Emergency level.	<i>alert</i>	Alert level.	<i>critical</i>	Critical level.	<i>error</i>	Error level.			
Option	Description													
<i>emergency</i>	Emergency level.													
<i>alert</i>	Alert level.													
<i>critical</i>	Critical level.													
<i>error</i>	Error level.													

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>warning</i>	Warning level.		
	<i>notification</i>	Notification level.		
	<i>information</i>	Information level.		
	<i>debug</i>	Debug level.		
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable sniffer traffic logging.		
	<i>disable</i>	Disable sniffer traffic logging.		
voip	Enable/disable VoIP logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable VoIP logging.		
	<i>disable</i>	Disable VoIP logging.		
ztna-traffic	Enable/disable ztna traffic logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable ztna traffic logging.		
	<i>disable</i>	Disable ztna traffic logging.		

\* This parameter may not exist in some models.

### config free-style

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
category	Log category.	option	-	traffic
	<b>Option</b>	<b>Description</b>		
	<i>traffic</i>	Traffic log.		

Parameter	Description	Type	Size	Default																																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>event</i></td><td>Event log.</td></tr><tr><td><i>virus</i></td><td>Antivirus log.</td></tr><tr><td><i>webfilter</i></td><td>Web filter log.</td></tr><tr><td><i>attack</i></td><td>Attack log.</td></tr><tr><td><i>spam</i></td><td>Antispam log.</td></tr><tr><td><i>anomaly</i></td><td>Anomaly log.</td></tr><tr><td><i>voip</i></td><td>VoIP log.</td></tr><tr><td><i>dlp</i></td><td>DLP log.</td></tr><tr><td><i>app-ctrl</i></td><td>Application control log.</td></tr><tr><td><i>waf</i></td><td>Web application firewall log.</td></tr><tr><td><i>dns</i></td><td>DNS detail log.</td></tr><tr><td><i>ssh</i></td><td>SSH log.</td></tr><tr><td><i>ssl</i></td><td>SSL log.</td></tr><tr><td><i>file-filter</i></td><td>File filter log.</td></tr><tr><td><i>icap</i></td><td>ICAP log.</td></tr></table>	Option	Description	<i>event</i>	Event log.	<i>virus</i>	Antivirus log.	<i>webfilter</i>	Web filter log.	<i>attack</i>	Attack log.	<i>spam</i>	Antispam log.	<i>anomaly</i>	Anomaly log.	<i>voip</i>	VoIP log.	<i>dlp</i>	DLP log.	<i>app-ctrl</i>	Application control log.	<i>waf</i>	Web application firewall log.	<i>dns</i>	DNS detail log.	<i>ssh</i>	SSH log.	<i>ssl</i>	SSL log.	<i>file-filter</i>	File filter log.	<i>icap</i>	ICAP log.			
	Option	Description																																		
	<i>event</i>	Event log.																																		
	<i>virus</i>	Antivirus log.																																		
	<i>webfilter</i>	Web filter log.																																		
	<i>attack</i>	Attack log.																																		
	<i>spam</i>	Antispam log.																																		
	<i>anomaly</i>	Anomaly log.																																		
	<i>voip</i>	VoIP log.																																		
	<i>dlp</i>	DLP log.																																		
	<i>app-ctrl</i>	Application control log.																																		
	<i>waf</i>	Web application firewall log.																																		
	<i>dns</i>	DNS detail log.																																		
	<i>ssh</i>	SSH log.																																		
	<i>ssl</i>	SSL log.																																		
	<i>file-filter</i>	File filter log.																																		
<i>icap</i>	ICAP log.																																			
filter	Free style filter string.	string	Maximum length: 1023																																	
filter-type	Include/exclude logs that match the filter.	option	-	include																																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>include</i></td><td>Include logs that match the filter.</td></tr><tr><td><i>exclude</i></td><td>Exclude logs that match the filter.</td></tr></table>	Option	Description	<i>include</i>	Include logs that match the filter.	<i>exclude</i>	Exclude logs that match the filter.																													
	Option	Description																																		
	<i>include</i>	Include logs that match the filter.																																		
<i>exclude</i>	Exclude logs that match the filter.																																			

### config log syslogd4 override-filter

Override filters for remote system server.

```
config log syslogd4 override-filter
  Description: Override filters for remote system server.
  set anomaly [enable|disable]
  set forward-traffic [enable|disable]
  config free-style
    Description: Free style filters.
    edit <id>
      set category [traffic|event|...]
      set filter {string}
```

```

        set filter-type [include|exclude]
    next
end
set gtp [enable|disable]
set local-traffic [enable|disable]
set multicast-traffic [enable|disable]
set severity [emergency|alert|...]
set sniffer-traffic [enable|disable]
set voip [enable|disable]
set ztna-traffic [enable|disable]
end

```

## config log syslogd4 override-filter

Parameter	Description	Type	Size	Default						
anomaly	Enable/disable anomaly logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable anomaly logging.</td></tr><tr><td><i>disable</i></td><td>Disable anomaly logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable anomaly logging.	<i>disable</i>	Disable anomaly logging.			
Option	Description									
<i>enable</i>	Enable anomaly logging.									
<i>disable</i>	Disable anomaly logging.									
forward-traffic	Enable/disable forward traffic logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable forward traffic logging.</td></tr><tr><td><i>disable</i></td><td>Disable forward traffic logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable forward traffic logging.	<i>disable</i>	Disable forward traffic logging.			
Option	Description									
<i>enable</i>	Enable forward traffic logging.									
<i>disable</i>	Disable forward traffic logging.									
gtp *	Enable/disable GTP messages logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable GTP messages logging.</td></tr><tr><td><i>disable</i></td><td>Disable GTP messages logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable GTP messages logging.	<i>disable</i>	Disable GTP messages logging.			
Option	Description									
<i>enable</i>	Enable GTP messages logging.									
<i>disable</i>	Disable GTP messages logging.									
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable local in or out traffic logging.</td></tr><tr><td><i>disable</i></td><td>Disable local in or out traffic logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable local in or out traffic logging.	<i>disable</i>	Disable local in or out traffic logging.			
Option	Description									
<i>enable</i>	Enable local in or out traffic logging.									
<i>disable</i>	Disable local in or out traffic logging.									
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable multicast traffic logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable multicast traffic logging.					
Option	Description									
<i>enable</i>	Enable multicast traffic logging.									

Parameter	Description	Type	Size	Default																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable multicast traffic logging.</td></tr></table>	Option	Description	<i>disable</i>	Disable multicast traffic logging.																	
	Option	Description																				
<i>disable</i>	Disable multicast traffic logging.																					
severity	Lowest severity level to log.	option	-	information																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>emergency</i></td><td>Emergency level.</td></tr><tr><td><i>alert</i></td><td>Alert level.</td></tr><tr><td><i>critical</i></td><td>Critical level.</td></tr><tr><td><i>error</i></td><td>Error level.</td></tr><tr><td><i>warning</i></td><td>Warning level.</td></tr><tr><td><i>notification</i></td><td>Notification level.</td></tr><tr><td><i>information</i></td><td>Information level.</td></tr><tr><td><i>debug</i></td><td>Debug level.</td></tr></table>	Option	Description	<i>emergency</i>	Emergency level.	<i>alert</i>	Alert level.	<i>critical</i>	Critical level.	<i>error</i>	Error level.	<i>warning</i>	Warning level.	<i>notification</i>	Notification level.	<i>information</i>	Information level.	<i>debug</i>	Debug level.			
	Option	Description																				
	<i>emergency</i>	Emergency level.																				
	<i>alert</i>	Alert level.																				
	<i>critical</i>	Critical level.																				
	<i>error</i>	Error level.																				
	<i>warning</i>	Warning level.																				
	<i>notification</i>	Notification level.																				
	<i>information</i>	Information level.																				
<i>debug</i>	Debug level.																					
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable sniffer traffic logging.</td></tr><tr><td><i>disable</i></td><td>Disable sniffer traffic logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable sniffer traffic logging.	<i>disable</i>	Disable sniffer traffic logging.															
	Option	Description																				
	<i>enable</i>	Enable sniffer traffic logging.																				
<i>disable</i>	Disable sniffer traffic logging.																					
voip	Enable/disable VoIP logging.	option	-	enable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable VoIP logging.</td></tr><tr><td><i>disable</i></td><td>Disable VoIP logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable VoIP logging.	<i>disable</i>	Disable VoIP logging.															
	Option	Description																				
	<i>enable</i>	Enable VoIP logging.																				
<i>disable</i>	Disable VoIP logging.																					
ztna-traffic	Enable/disable ztna traffic logging.	option	-	enable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable ztna traffic logging.</td></tr><tr><td><i>disable</i></td><td>Disable ztna traffic logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable ztna traffic logging.	<i>disable</i>	Disable ztna traffic logging.															
	Option	Description																				
	<i>enable</i>	Enable ztna traffic logging.																				
<i>disable</i>	Disable ztna traffic logging.																					

\* This parameter may not exist in some models.

## config free-style

Parameter	Description	Type	Size	Default																																		
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0																																		
category	Log category.	option	-	traffic																																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>traffic</td><td>Traffic log.</td></tr><tr><td>event</td><td>Event log.</td></tr><tr><td>virus</td><td>Antivirus log.</td></tr><tr><td>webfilter</td><td>Web filter log.</td></tr><tr><td>attack</td><td>Attack log.</td></tr><tr><td>spam</td><td>Antispam log.</td></tr><tr><td>anomaly</td><td>Anomaly log.</td></tr><tr><td>voip</td><td>VoIP log.</td></tr><tr><td>dlp</td><td>DLP log.</td></tr><tr><td>app-ctrl</td><td>Application control log.</td></tr><tr><td>waf</td><td>Web application firewall log.</td></tr><tr><td>dns</td><td>DNS detail log.</td></tr><tr><td>ssh</td><td>SSH log.</td></tr><tr><td>ssl</td><td>SSL log.</td></tr><tr><td>file-filter</td><td>File filter log.</td></tr><tr><td>icap</td><td>ICAP log.</td></tr></table>	Option	Description	traffic	Traffic log.	event	Event log.	virus	Antivirus log.	webfilter	Web filter log.	attack	Attack log.	spam	Antispam log.	anomaly	Anomaly log.	voip	VoIP log.	dlp	DLP log.	app-ctrl	Application control log.	waf	Web application firewall log.	dns	DNS detail log.	ssh	SSH log.	ssl	SSL log.	file-filter	File filter log.	icap	ICAP log.			
	Option	Description																																				
	traffic	Traffic log.																																				
	event	Event log.																																				
	virus	Antivirus log.																																				
	webfilter	Web filter log.																																				
	attack	Attack log.																																				
	spam	Antispam log.																																				
	anomaly	Anomaly log.																																				
	voip	VoIP log.																																				
	dlp	DLP log.																																				
	app-ctrl	Application control log.																																				
	waf	Web application firewall log.																																				
	dns	DNS detail log.																																				
	ssh	SSH log.																																				
	ssl	SSL log.																																				
	file-filter	File filter log.																																				
icap	ICAP log.																																					
filter	Free style filter string.	string	Maximum length: 1023																																			
filter-type	Include/exclude logs that match the filter.	option	-	include																																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>include</td><td>Include logs that match the filter.</td></tr><tr><td>exclude</td><td>Exclude logs that match the filter.</td></tr></table>	Option	Description	include	Include logs that match the filter.	exclude	Exclude logs that match the filter.																															
	Option	Description																																				
	include	Include logs that match the filter.																																				
exclude	Exclude logs that match the filter.																																					

## config log syslogd4 override-setting

Override settings for remote syslog server.

```
config log syslogd4 override-setting
  Description: Override settings for remote syslog server.
  set certificate {string}
  config custom-field-name
    Description: Custom field name for CEF format logging.
    edit <id>
      set name {string}
      set custom {string}
    next
  end
  set enc-algorithm [high-medium|high|...]
  set facility [kernel|user|...]
  set format [default|csv|...]
  set interface {string}
  set interface-select-method [auto|sdwan|...]
  set max-log-rate {integer}
  set mode [udp|legacy-reliable|...]
  set port {integer}
  set priority [default|low]
  set server {string}
  set source-ip {string}
  set ssl-min-proto-version [default|SSLv3|...]
  set status [enable|disable]
end
```

## config log syslogd4 override-setting

Parameter	Description	Type	Size	Default
certificate	Certificate used to communicate with Syslog server.	string	Maximum length: 35	
enc-algorithm	Enable/disable reliable syslogging with TLS encryption.	option	-	disable
	<div>OptionDescription</div>			
	high-medium	SSL communication with high and medium encryption algorithms.		
	high	SSL communication with high encryption algorithms.		
	low	SSL communication with low encryption algorithms.		
	disable	Disable SSL communication.		
facility	Remote syslog facility.	option	-	local7
	<div>OptionDescription</div>			
	kernel	Kernel messages.		



Parameter	Description	Type	Size	Default																																																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>user</i></td><td>Random user-level messages.</td></tr><tr><td><i>mail</i></td><td>Mail system.</td></tr><tr><td><i>daemon</i></td><td>System daemons.</td></tr><tr><td><i>auth</i></td><td>Security/authorization messages.</td></tr><tr><td><i>syslog</i></td><td>Messages generated internally by syslog.</td></tr><tr><td><i>lpr</i></td><td>Line printer subsystem.</td></tr><tr><td><i>news</i></td><td>Network news subsystem.</td></tr><tr><td><i>uucp</i></td><td>Network news subsystem.</td></tr><tr><td><i>cron</i></td><td>Clock daemon.</td></tr><tr><td><i>authpriv</i></td><td>Security/authorization messages (private).</td></tr><tr><td><i>ftp</i></td><td>FTP daemon.</td></tr><tr><td><i>ntp</i></td><td>NTP daemon.</td></tr><tr><td><i>audit</i></td><td>Log audit.</td></tr><tr><td><i>alert</i></td><td>Log alert.</td></tr><tr><td><i>clock</i></td><td>Clock daemon.</td></tr><tr><td><i>local0</i></td><td>Reserved for local use.</td></tr><tr><td><i>local1</i></td><td>Reserved for local use.</td></tr><tr><td><i>local2</i></td><td>Reserved for local use.</td></tr><tr><td><i>local3</i></td><td>Reserved for local use.</td></tr><tr><td><i>local4</i></td><td>Reserved for local use.</td></tr><tr><td><i>local5</i></td><td>Reserved for local use.</td></tr><tr><td><i>local6</i></td><td>Reserved for local use.</td></tr><tr><td><i>local7</i></td><td>Reserved for local use.</td></tr></table>	Option	Description	<i>user</i>	Random user-level messages.	<i>mail</i>	Mail system.	<i>daemon</i>	System daemons.	<i>auth</i>	Security/authorization messages.	<i>syslog</i>	Messages generated internally by syslog.	<i>lpr</i>	Line printer subsystem.	<i>news</i>	Network news subsystem.	<i>uucp</i>	Network news subsystem.	<i>cron</i>	Clock daemon.	<i>authpriv</i>	Security/authorization messages (private).	<i>ftp</i>	FTP daemon.	<i>ntp</i>	NTP daemon.	<i>audit</i>	Log audit.	<i>alert</i>	Log alert.	<i>clock</i>	Clock daemon.	<i>local0</i>	Reserved for local use.	<i>local1</i>	Reserved for local use.	<i>local2</i>	Reserved for local use.	<i>local3</i>	Reserved for local use.	<i>local4</i>	Reserved for local use.	<i>local5</i>	Reserved for local use.	<i>local6</i>	Reserved for local use.	<i>local7</i>	Reserved for local use.			
	Option	Description																																																		
	<i>user</i>	Random user-level messages.																																																		
	<i>mail</i>	Mail system.																																																		
	<i>daemon</i>	System daemons.																																																		
	<i>auth</i>	Security/authorization messages.																																																		
	<i>syslog</i>	Messages generated internally by syslog.																																																		
	<i>lpr</i>	Line printer subsystem.																																																		
	<i>news</i>	Network news subsystem.																																																		
	<i>uucp</i>	Network news subsystem.																																																		
	<i>cron</i>	Clock daemon.																																																		
	<i>authpriv</i>	Security/authorization messages (private).																																																		
	<i>ftp</i>	FTP daemon.																																																		
	<i>ntp</i>	NTP daemon.																																																		
	<i>audit</i>	Log audit.																																																		
	<i>alert</i>	Log alert.																																																		
	<i>clock</i>	Clock daemon.																																																		
	<i>local0</i>	Reserved for local use.																																																		
	<i>local1</i>	Reserved for local use.																																																		
	<i>local2</i>	Reserved for local use.																																																		
	<i>local3</i>	Reserved for local use.																																																		
	<i>local4</i>	Reserved for local use.																																																		
	<i>local5</i>	Reserved for local use.																																																		
<i>local6</i>	Reserved for local use.																																																			
<i>local7</i>	Reserved for local use.																																																			
format	Log format.	option	-	default																																																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>Syslog format.</td></tr><tr><td><i>csv</i></td><td>CSV (Comma Separated Values) format.</td></tr><tr><td><i>cef</i></td><td>CEF (Common Event Format) format.</td></tr><tr><td><i>rfc5424</i></td><td>Syslog RFC5424 format.</td></tr></table>	Option	Description	<i>default</i>	Syslog format.	<i>csv</i>	CSV (Comma Separated Values) format.	<i>cef</i>	CEF (Common Event Format) format.	<i>rfc5424</i>	Syslog RFC5424 format.																																									
	Option	Description																																																		
	<i>default</i>	Syslog format.																																																		
	<i>csv</i>	CSV (Comma Separated Values) format.																																																		
	<i>cef</i>	CEF (Common Event Format) format.																																																		
<i>rfc5424</i>	Syslog RFC5424 format.																																																			

Parameter	Description	Type	Size	Default								
interface	Specify outgoing interface to reach server.	string	Maximum length: 15									
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>auto</td><td>Set outgoing interface automatically.</td></tr><tr><td>sdwan</td><td>Set outgoing interface by SD-WAN or policy routing rules.</td></tr><tr><td>specify</td><td>Set outgoing interface manually.</td></tr></table>	Option	Description	auto	Set outgoing interface automatically.	sdwan	Set outgoing interface by SD-WAN or policy routing rules.	specify	Set outgoing interface manually.			
Option	Description											
auto	Set outgoing interface automatically.											
sdwan	Set outgoing interface by SD-WAN or policy routing rules.											
specify	Set outgoing interface manually.											
max-log-rate	Syslog maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0								
mode	Remote syslog logging over UDP/Reliable TCP.	option	-	udp								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>udp</td><td>Enable syslogging over UDP.</td></tr><tr><td>legacy-reliable</td><td>Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).</td></tr><tr><td>reliable</td><td>Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).</td></tr></table>	Option	Description	udp	Enable syslogging over UDP.	legacy-reliable	Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).	reliable	Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).			
Option	Description											
udp	Enable syslogging over UDP.											
legacy-reliable	Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).											
reliable	Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).											
port	Server listen port.	integer	Minimum value: 0 Maximum value: 65535	514								
priority	Set log transmission priority.	option	-	default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>default</td><td>Set Syslog transmission priority to default.</td></tr><tr><td>low</td><td>Set Syslog transmission priority to low.</td></tr></table>	Option	Description	default	Set Syslog transmission priority to default.	low	Set Syslog transmission priority to low.					
Option	Description											
default	Set Syslog transmission priority to default.											
low	Set Syslog transmission priority to low.											
server	Address of remote syslog server.	string	Maximum length: 127									
source-ip	Source IP address of syslog.	string	Maximum length: 63									
ssl-min-protocol-version	Minimum supported protocol version for SSL/TLS connections.	option	-	default								

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>default</i>	Follow system global setting.		
	<i>SSLv3</i>	SSLv3.		
	<i>TLSv1</i>	TLSv1.		
	<i>TLSv1-1</i>	TLSv1.1.		
	<i>TLSv1-2</i>	TLSv1.2.		
status	Enable/disable remote syslog logging.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Log to remote syslog server.		
	<i>disable</i>	Do not log to remote syslog server.		

### config custom-field-name

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 255	0
name	Field name.	string	Maximum length: 35	
custom	Field custom name.	string	Maximum length: 35	

## config log syslogd4 setting

Global settings for remote syslog server.

```
config log syslogd4 setting
    Description: Global settings for remote syslog server.
    set certificate {string}
    config custom-field-name
        Description: Custom field name for CEF format logging.
        edit <id>
            set name {string}
            set custom {string}
        next
    end
    set enc-algorithm [high-medium|high|...]
    set facility [kernel|user|...]
    set format [default|csv|...]
```

```

set interface {string}
set interface-select-method [auto|sdwan|...]
set max-log-rate {integer}
set mode [udp|legacy-reliable|...]
set port {integer}
set priority [default|low]
set server {string}
set source-ip {string}
set ssl-min-proto-version [default|SSLv3|...]
set status [enable|disable]
end

```

end

## config log syslogd4 setting

Parameter	Description	Type	Size	Default
certificate	Certificate used to communicate with Syslog server.	string	Maximum length: 35	
enc-algorithm	Enable/disable reliable syslogging with TLS encryption.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>high-medium</i>	SSL communication with high and medium encryption algorithms.		
	<i>high</i>	SSL communication with high encryption algorithms.		
	<i>low</i>	SSL communication with low encryption algorithms.		
	<i>disable</i>	Disable SSL communication.		
facility	Remote syslog facility.	option	-	local7
	<b>Option</b>	<b>Description</b>		
	<i>kernel</i>	Kernel messages.		
	<i>user</i>	Random user-level messages.		
	<i>mail</i>	Mail system.		
	<i>daemon</i>	System daemons.		
	<i>auth</i>	Security/authorization messages.		
	<i>syslog</i>	Messages generated internally by syslog.		
	<i>lpr</i>	Line printer subsystem.		
	<i>news</i>	Network news subsystem.		
	<i>uucp</i>	Network news subsystem.		
	<i>cron</i>	Clock daemon.		
	<i>authpriv</i>	Security/authorization messages (private).		
	<i>ftp</i>	FTP daemon.		

Parameter	Description	Type	Size	Default																										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ntp</i></td><td>NTP daemon.</td></tr><tr><td><i>audit</i></td><td>Log audit.</td></tr><tr><td><i>alert</i></td><td>Log alert.</td></tr><tr><td><i>clock</i></td><td>Clock daemon.</td></tr><tr><td><i>local0</i></td><td>Reserved for local use.</td></tr><tr><td><i>local1</i></td><td>Reserved for local use.</td></tr><tr><td><i>local2</i></td><td>Reserved for local use.</td></tr><tr><td><i>local3</i></td><td>Reserved for local use.</td></tr><tr><td><i>local4</i></td><td>Reserved for local use.</td></tr><tr><td><i>local5</i></td><td>Reserved for local use.</td></tr><tr><td><i>local6</i></td><td>Reserved for local use.</td></tr><tr><td><i>local7</i></td><td>Reserved for local use.</td></tr></table>	Option	Description	<i>ntp</i>	NTP daemon.	<i>audit</i>	Log audit.	<i>alert</i>	Log alert.	<i>clock</i>	Clock daemon.	<i>local0</i>	Reserved for local use.	<i>local1</i>	Reserved for local use.	<i>local2</i>	Reserved for local use.	<i>local3</i>	Reserved for local use.	<i>local4</i>	Reserved for local use.	<i>local5</i>	Reserved for local use.	<i>local6</i>	Reserved for local use.	<i>local7</i>	Reserved for local use.			
	Option	Description																												
	<i>ntp</i>	NTP daemon.																												
	<i>audit</i>	Log audit.																												
	<i>alert</i>	Log alert.																												
	<i>clock</i>	Clock daemon.																												
	<i>local0</i>	Reserved for local use.																												
	<i>local1</i>	Reserved for local use.																												
	<i>local2</i>	Reserved for local use.																												
	<i>local3</i>	Reserved for local use.																												
	<i>local4</i>	Reserved for local use.																												
	<i>local5</i>	Reserved for local use.																												
	<i>local6</i>	Reserved for local use.																												
<i>local7</i>	Reserved for local use.																													
format	Log format.	option	-	default																										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>Syslog format.</td></tr><tr><td><i>csv</i></td><td>CSV (Comma Separated Values) format.</td></tr><tr><td><i>cef</i></td><td>CEF (Common Event Format) format.</td></tr><tr><td><i>rfc5424</i></td><td>Syslog RFC5424 format.</td></tr></table>	Option	Description	<i>default</i>	Syslog format.	<i>csv</i>	CSV (Comma Separated Values) format.	<i>cef</i>	CEF (Common Event Format) format.	<i>rfc5424</i>	Syslog RFC5424 format.																			
	Option	Description																												
	<i>default</i>	Syslog format.																												
	<i>csv</i>	CSV (Comma Separated Values) format.																												
	<i>cef</i>	CEF (Common Event Format) format.																												
<i>rfc5424</i>	Syslog RFC5424 format.																													
interface	Specify outgoing interface to reach server.	string	Maximum length: 15																											
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto																										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto</i></td><td>Set outgoing interface automatically.</td></tr><tr><td><i>sdwan</i></td><td>Set outgoing interface by SD-WAN or policy routing rules.</td></tr><tr><td><i>specify</i></td><td>Set outgoing interface manually.</td></tr></table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.																					
	Option	Description																												
	<i>auto</i>	Set outgoing interface automatically.																												
	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.																												
<i>specify</i>	Set outgoing interface manually.																													

Parameter	Description	Type	Size	Default
max-log-rate	Syslog maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0
mode	Remote syslog logging over UDP/Reliable TCP.	option	-	udp
	<b>Option</b>	<b>Description</b>		
	udp	Enable syslogging over UDP.		
	legacy-reliable	Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).		
	reliable	Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).		
port	Server listen port.	integer	Minimum value: 0 Maximum value: 65535	514
priority	Set log transmission priority.	option	-	default
	<b>Option</b>	<b>Description</b>		
	default	Set Syslog transmission priority to default.		
	low	Set Syslog transmission priority to low.		
server	Address of remote syslog server.	string	Maximum length: 127	
source-ip	Source IP address of syslog.	string	Maximum length: 63	
ssl-min-protocol-version	Minimum supported protocol version for SSL/TLS connections.	option	-	default
	<b>Option</b>	<b>Description</b>		
	default	Follow system global setting.		
	SSLv3	SSLv3.		
	TLSv1	TLSv1.		
	TLSv1-1	TLSv1.1.		
	TLSv1-2	TLSv1.2.		
status	Enable/disable remote syslog logging.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>enable</i>	Log to remote syslog server.		
	<i>disable</i>	Do not log to remote syslog server.		

### config custom-field-name

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 255	0
name	Field name.	string	Maximum length: 35	
custom	Field custom name.	string	Maximum length: 35	

### config log syslogd filter

Filters for remote system server.

```

config log syslogd filter
    Description: Filters for remote system server.
    set anomaly [enable|disable]
    set forward-traffic [enable|disable]
    config free-style
        Description: Free style filters.
        edit <id>
            set category [traffic|event|...]
            set filter {string}
            set filter-type [include|exclude]
        next
    end
    set gtp [enable|disable]
    set local-traffic [enable|disable]
    set multicast-traffic [enable|disable]
    set severity [emergency|alert|...]
    set sniffer-traffic [enable|disable]
    set voip [enable|disable]
    set ztna-traffic [enable|disable]
end

```

## config log syslogd filter

Parameter	Description	Type	Size	Default										
anomaly	Enable/disable anomaly logging.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable anomaly logging.</td></tr><tr><td><i>disable</i></td><td>Disable anomaly logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable anomaly logging.	<i>disable</i>	Disable anomaly logging.							
Option	Description													
<i>enable</i>	Enable anomaly logging.													
<i>disable</i>	Disable anomaly logging.													
forward-traffic	Enable/disable forward traffic logging.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable forward traffic logging.</td></tr><tr><td><i>disable</i></td><td>Disable forward traffic logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable forward traffic logging.	<i>disable</i>	Disable forward traffic logging.							
Option	Description													
<i>enable</i>	Enable forward traffic logging.													
<i>disable</i>	Disable forward traffic logging.													
gtp *	Enable/disable GTP messages logging.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable GTP messages logging.</td></tr><tr><td><i>disable</i></td><td>Disable GTP messages logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable GTP messages logging.	<i>disable</i>	Disable GTP messages logging.							
Option	Description													
<i>enable</i>	Enable GTP messages logging.													
<i>disable</i>	Disable GTP messages logging.													
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable local in or out traffic logging.</td></tr><tr><td><i>disable</i></td><td>Disable local in or out traffic logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable local in or out traffic logging.	<i>disable</i>	Disable local in or out traffic logging.							
Option	Description													
<i>enable</i>	Enable local in or out traffic logging.													
<i>disable</i>	Disable local in or out traffic logging.													
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable multicast traffic logging.</td></tr><tr><td><i>disable</i></td><td>Disable multicast traffic logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable multicast traffic logging.	<i>disable</i>	Disable multicast traffic logging.							
Option	Description													
<i>enable</i>	Enable multicast traffic logging.													
<i>disable</i>	Disable multicast traffic logging.													
severity	Lowest severity level to log.	option	-	information										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>emergency</i></td><td>Emergency level.</td></tr><tr><td><i>alert</i></td><td>Alert level.</td></tr><tr><td><i>critical</i></td><td>Critical level.</td></tr><tr><td><i>error</i></td><td>Error level.</td></tr></table>	Option	Description	<i>emergency</i>	Emergency level.	<i>alert</i>	Alert level.	<i>critical</i>	Critical level.	<i>error</i>	Error level.			
Option	Description													
<i>emergency</i>	Emergency level.													
<i>alert</i>	Alert level.													
<i>critical</i>	Critical level.													
<i>error</i>	Error level.													



Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>warning</i>	Warning level.		
	<i>notification</i>	Notification level.		
	<i>information</i>	Information level.		
	<i>debug</i>	Debug level.		
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable sniffer traffic logging.		
	<i>disable</i>	Disable sniffer traffic logging.		
voip	Enable/disable VoIP logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable VoIP logging.		
	<i>disable</i>	Disable VoIP logging.		
ztna-traffic	Enable/disable ztna traffic logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable ztna traffic logging.		
	<i>disable</i>	Disable ztna traffic logging.		

\* This parameter may not exist in some models.

### config free-style

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
category	Log category.	option	-	traffic
	<b>Option</b>	<b>Description</b>		
	<i>traffic</i>	Traffic log.		

Parameter	Description	Type	Size	Default																																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>event</i></td><td>Event log.</td></tr><tr><td><i>virus</i></td><td>Antivirus log.</td></tr><tr><td><i>webfilter</i></td><td>Web filter log.</td></tr><tr><td><i>attack</i></td><td>Attack log.</td></tr><tr><td><i>spam</i></td><td>Antispam log.</td></tr><tr><td><i>anomaly</i></td><td>Anomaly log.</td></tr><tr><td><i>voip</i></td><td>VoIP log.</td></tr><tr><td><i>dlp</i></td><td>DLP log.</td></tr><tr><td><i>app-ctrl</i></td><td>Application control log.</td></tr><tr><td><i>waf</i></td><td>Web application firewall log.</td></tr><tr><td><i>dns</i></td><td>DNS detail log.</td></tr><tr><td><i>ssh</i></td><td>SSH log.</td></tr><tr><td><i>ssl</i></td><td>SSL log.</td></tr><tr><td><i>file-filter</i></td><td>File filter log.</td></tr><tr><td><i>icap</i></td><td>ICAP log.</td></tr></table>	Option	Description	<i>event</i>	Event log.	<i>virus</i>	Antivirus log.	<i>webfilter</i>	Web filter log.	<i>attack</i>	Attack log.	<i>spam</i>	Antispam log.	<i>anomaly</i>	Anomaly log.	<i>voip</i>	VoIP log.	<i>dlp</i>	DLP log.	<i>app-ctrl</i>	Application control log.	<i>waf</i>	Web application firewall log.	<i>dns</i>	DNS detail log.	<i>ssh</i>	SSH log.	<i>ssl</i>	SSL log.	<i>file-filter</i>	File filter log.	<i>icap</i>	ICAP log.			
	Option	Description																																		
	<i>event</i>	Event log.																																		
	<i>virus</i>	Antivirus log.																																		
	<i>webfilter</i>	Web filter log.																																		
	<i>attack</i>	Attack log.																																		
	<i>spam</i>	Antispam log.																																		
	<i>anomaly</i>	Anomaly log.																																		
	<i>voip</i>	VoIP log.																																		
	<i>dlp</i>	DLP log.																																		
	<i>app-ctrl</i>	Application control log.																																		
	<i>waf</i>	Web application firewall log.																																		
	<i>dns</i>	DNS detail log.																																		
	<i>ssh</i>	SSH log.																																		
	<i>ssl</i>	SSL log.																																		
	<i>file-filter</i>	File filter log.																																		
<i>icap</i>	ICAP log.																																			
filter	Free style filter string.	string	Maximum length: 1023																																	
filter-type	Include/exclude logs that match the filter.	option	-	include																																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>include</i></td><td>Include logs that match the filter.</td></tr><tr><td><i>exclude</i></td><td>Exclude logs that match the filter.</td></tr></table>	Option	Description	<i>include</i>	Include logs that match the filter.	<i>exclude</i>	Exclude logs that match the filter.																													
	Option	Description																																		
	<i>include</i>	Include logs that match the filter.																																		
<i>exclude</i>	Exclude logs that match the filter.																																			

### config log syslogd override-filter

Override filters for remote system server.

```

config log syslogd override-filter
  Description: Override filters for remote system server.
  set anomaly [enable|disable]
  set forward-traffic [enable|disable]
  config free-style
    Description: Free style filters.
    edit <id>
      set category [traffic|event|...]
      set filter {string}

```

```

        set filter-type [include|exclude]
    next
end
set gtp [enable|disable]
set local-traffic [enable|disable]
set multicast-traffic [enable|disable]
set severity [emergency|alert|...]
set sniffer-traffic [enable|disable]
set voip [enable|disable]
set ztna-traffic [enable|disable]
end

```

## config log syslogd override-filter

Parameter	Description	Type	Size	Default						
anomaly	Enable/disable anomaly logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable anomaly logging.</td></tr><tr><td><i>disable</i></td><td>Disable anomaly logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable anomaly logging.	<i>disable</i>	Disable anomaly logging.			
Option	Description									
<i>enable</i>	Enable anomaly logging.									
<i>disable</i>	Disable anomaly logging.									
forward-traffic	Enable/disable forward traffic logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable forward traffic logging.</td></tr><tr><td><i>disable</i></td><td>Disable forward traffic logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable forward traffic logging.	<i>disable</i>	Disable forward traffic logging.			
Option	Description									
<i>enable</i>	Enable forward traffic logging.									
<i>disable</i>	Disable forward traffic logging.									
gtp *	Enable/disable GTP messages logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable GTP messages logging.</td></tr><tr><td><i>disable</i></td><td>Disable GTP messages logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable GTP messages logging.	<i>disable</i>	Disable GTP messages logging.			
Option	Description									
<i>enable</i>	Enable GTP messages logging.									
<i>disable</i>	Disable GTP messages logging.									
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable local in or out traffic logging.</td></tr><tr><td><i>disable</i></td><td>Disable local in or out traffic logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable local in or out traffic logging.	<i>disable</i>	Disable local in or out traffic logging.			
Option	Description									
<i>enable</i>	Enable local in or out traffic logging.									
<i>disable</i>	Disable local in or out traffic logging.									
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable multicast traffic logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable multicast traffic logging.					
Option	Description									
<i>enable</i>	Enable multicast traffic logging.									

Parameter	Description	Type	Size	Default																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable multicast traffic logging.</td></tr></table>	Option	Description	<i>disable</i>	Disable multicast traffic logging.																	
	Option	Description																				
<i>disable</i>	Disable multicast traffic logging.																					
severity	Lowest severity level to log.	option	-	information																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>emergency</i></td><td>Emergency level.</td></tr><tr><td><i>alert</i></td><td>Alert level.</td></tr><tr><td><i>critical</i></td><td>Critical level.</td></tr><tr><td><i>error</i></td><td>Error level.</td></tr><tr><td><i>warning</i></td><td>Warning level.</td></tr><tr><td><i>notification</i></td><td>Notification level.</td></tr><tr><td><i>information</i></td><td>Information level.</td></tr><tr><td><i>debug</i></td><td>Debug level.</td></tr></table>	Option	Description	<i>emergency</i>	Emergency level.	<i>alert</i>	Alert level.	<i>critical</i>	Critical level.	<i>error</i>	Error level.	<i>warning</i>	Warning level.	<i>notification</i>	Notification level.	<i>information</i>	Information level.	<i>debug</i>	Debug level.			
	Option	Description																				
	<i>emergency</i>	Emergency level.																				
	<i>alert</i>	Alert level.																				
	<i>critical</i>	Critical level.																				
	<i>error</i>	Error level.																				
	<i>warning</i>	Warning level.																				
	<i>notification</i>	Notification level.																				
	<i>information</i>	Information level.																				
<i>debug</i>	Debug level.																					
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable sniffer traffic logging.</td></tr><tr><td><i>disable</i></td><td>Disable sniffer traffic logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable sniffer traffic logging.	<i>disable</i>	Disable sniffer traffic logging.															
	Option	Description																				
	<i>enable</i>	Enable sniffer traffic logging.																				
<i>disable</i>	Disable sniffer traffic logging.																					
voip	Enable/disable VoIP logging.	option	-	enable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable VoIP logging.</td></tr><tr><td><i>disable</i></td><td>Disable VoIP logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable VoIP logging.	<i>disable</i>	Disable VoIP logging.															
	Option	Description																				
	<i>enable</i>	Enable VoIP logging.																				
<i>disable</i>	Disable VoIP logging.																					
ztna-traffic	Enable/disable ztna traffic logging.	option	-	enable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable ztna traffic logging.</td></tr><tr><td><i>disable</i></td><td>Disable ztna traffic logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable ztna traffic logging.	<i>disable</i>	Disable ztna traffic logging.															
	Option	Description																				
	<i>enable</i>	Enable ztna traffic logging.																				
<i>disable</i>	Disable ztna traffic logging.																					

\* This parameter may not exist in some models.

## config free-style

Parameter	Description	Type	Size	Default																																		
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0																																		
category	Log category.	option	-	traffic																																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>traffic</td><td>Traffic log.</td></tr><tr><td>event</td><td>Event log.</td></tr><tr><td>virus</td><td>Antivirus log.</td></tr><tr><td>webfilter</td><td>Web filter log.</td></tr><tr><td>attack</td><td>Attack log.</td></tr><tr><td>spam</td><td>Antispam log.</td></tr><tr><td>anomaly</td><td>Anomaly log.</td></tr><tr><td>voip</td><td>VoIP log.</td></tr><tr><td>dlp</td><td>DLP log.</td></tr><tr><td>app-ctrl</td><td>Application control log.</td></tr><tr><td>waf</td><td>Web application firewall log.</td></tr><tr><td>dns</td><td>DNS detail log.</td></tr><tr><td>ssh</td><td>SSH log.</td></tr><tr><td>ssl</td><td>SSL log.</td></tr><tr><td>file-filter</td><td>File filter log.</td></tr><tr><td>icap</td><td>ICAP log.</td></tr></table>	Option	Description	traffic	Traffic log.	event	Event log.	virus	Antivirus log.	webfilter	Web filter log.	attack	Attack log.	spam	Antispam log.	anomaly	Anomaly log.	voip	VoIP log.	dlp	DLP log.	app-ctrl	Application control log.	waf	Web application firewall log.	dns	DNS detail log.	ssh	SSH log.	ssl	SSL log.	file-filter	File filter log.	icap	ICAP log.			
	Option	Description																																				
	traffic	Traffic log.																																				
	event	Event log.																																				
	virus	Antivirus log.																																				
	webfilter	Web filter log.																																				
	attack	Attack log.																																				
	spam	Antispam log.																																				
	anomaly	Anomaly log.																																				
	voip	VoIP log.																																				
	dlp	DLP log.																																				
	app-ctrl	Application control log.																																				
	waf	Web application firewall log.																																				
	dns	DNS detail log.																																				
	ssh	SSH log.																																				
	ssl	SSL log.																																				
	file-filter	File filter log.																																				
icap	ICAP log.																																					
filter	Free style filter string.	string	Maximum length: 1023																																			
filter-type	Include/exclude logs that match the filter.	option	-	include																																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>include</td><td>Include logs that match the filter.</td></tr><tr><td>exclude</td><td>Exclude logs that match the filter.</td></tr></table>	Option	Description	include	Include logs that match the filter.	exclude	Exclude logs that match the filter.																															
	Option	Description																																				
	include	Include logs that match the filter.																																				
exclude	Exclude logs that match the filter.																																					

## config log syslogd override-setting

Override settings for remote syslog server.

```
config log syslogd override-setting
  Description: Override settings for remote syslog server.
  set certificate {string}
  config custom-field-name
    Description: Custom field name for CEF format logging.
    edit <id>
      set name {string}
      set custom {string}
    next
  end
  set enc-algorithm [high-medium|high|...]
  set facility [kernel|user|...]
  set format [default|csv|...]
  set interface {string}
  set interface-select-method [auto|sdwan|...]
  set max-log-rate {integer}
  set mode [udp|legacy-reliable|...]
  set port {integer}
  set priority [default|low]
  set server {string}
  set source-ip {string}
  set ssl-min-proto-version [default|SSLv3|...]
  set status [enable|disable]
end
```

## config log syslogd override-setting

Parameter	Description	Type	Size	Default
certificate	Certificate used to communicate with Syslog server.	string	Maximum length: 35	
enc-algorithm	Enable/disable reliable syslogging with TLS encryption.	option	-	disable
	<div><div>Option</div><div>Description</div></div>			
	high-medium	SSL communication with high and medium encryption algorithms.		
	high	SSL communication with high encryption algorithms.		
	low	SSL communication with low encryption algorithms.		
	disable	Disable SSL communication.		
facility	Remote syslog facility.	option	-	local7
	<div><div>Option</div><div>Description</div></div>			
	kernel	Kernel messages.		

Parameter	Description	Type	Size	Default																																																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>user</i></td><td>Random user-level messages.</td></tr><tr><td><i>mail</i></td><td>Mail system.</td></tr><tr><td><i>daemon</i></td><td>System daemons.</td></tr><tr><td><i>auth</i></td><td>Security/authorization messages.</td></tr><tr><td><i>syslog</i></td><td>Messages generated internally by syslog.</td></tr><tr><td><i>lpr</i></td><td>Line printer subsystem.</td></tr><tr><td><i>news</i></td><td>Network news subsystem.</td></tr><tr><td><i>uucp</i></td><td>Network news subsystem.</td></tr><tr><td><i>cron</i></td><td>Clock daemon.</td></tr><tr><td><i>authpriv</i></td><td>Security/authorization messages (private).</td></tr><tr><td><i>ftp</i></td><td>FTP daemon.</td></tr><tr><td><i>ntp</i></td><td>NTP daemon.</td></tr><tr><td><i>audit</i></td><td>Log audit.</td></tr><tr><td><i>alert</i></td><td>Log alert.</td></tr><tr><td><i>clock</i></td><td>Clock daemon.</td></tr><tr><td><i>local0</i></td><td>Reserved for local use.</td></tr><tr><td><i>local1</i></td><td>Reserved for local use.</td></tr><tr><td><i>local2</i></td><td>Reserved for local use.</td></tr><tr><td><i>local3</i></td><td>Reserved for local use.</td></tr><tr><td><i>local4</i></td><td>Reserved for local use.</td></tr><tr><td><i>local5</i></td><td>Reserved for local use.</td></tr><tr><td><i>local6</i></td><td>Reserved for local use.</td></tr><tr><td><i>local7</i></td><td>Reserved for local use.</td></tr></table>	Option	Description	<i>user</i>	Random user-level messages.	<i>mail</i>	Mail system.	<i>daemon</i>	System daemons.	<i>auth</i>	Security/authorization messages.	<i>syslog</i>	Messages generated internally by syslog.	<i>lpr</i>	Line printer subsystem.	<i>news</i>	Network news subsystem.	<i>uucp</i>	Network news subsystem.	<i>cron</i>	Clock daemon.	<i>authpriv</i>	Security/authorization messages (private).	<i>ftp</i>	FTP daemon.	<i>ntp</i>	NTP daemon.	<i>audit</i>	Log audit.	<i>alert</i>	Log alert.	<i>clock</i>	Clock daemon.	<i>local0</i>	Reserved for local use.	<i>local1</i>	Reserved for local use.	<i>local2</i>	Reserved for local use.	<i>local3</i>	Reserved for local use.	<i>local4</i>	Reserved for local use.	<i>local5</i>	Reserved for local use.	<i>local6</i>	Reserved for local use.	<i>local7</i>	Reserved for local use.			
	Option	Description																																																		
	<i>user</i>	Random user-level messages.																																																		
	<i>mail</i>	Mail system.																																																		
	<i>daemon</i>	System daemons.																																																		
	<i>auth</i>	Security/authorization messages.																																																		
	<i>syslog</i>	Messages generated internally by syslog.																																																		
	<i>lpr</i>	Line printer subsystem.																																																		
	<i>news</i>	Network news subsystem.																																																		
	<i>uucp</i>	Network news subsystem.																																																		
	<i>cron</i>	Clock daemon.																																																		
	<i>authpriv</i>	Security/authorization messages (private).																																																		
	<i>ftp</i>	FTP daemon.																																																		
	<i>ntp</i>	NTP daemon.																																																		
	<i>audit</i>	Log audit.																																																		
	<i>alert</i>	Log alert.																																																		
	<i>clock</i>	Clock daemon.																																																		
	<i>local0</i>	Reserved for local use.																																																		
	<i>local1</i>	Reserved for local use.																																																		
	<i>local2</i>	Reserved for local use.																																																		
	<i>local3</i>	Reserved for local use.																																																		
	<i>local4</i>	Reserved for local use.																																																		
	<i>local5</i>	Reserved for local use.																																																		
<i>local6</i>	Reserved for local use.																																																			
<i>local7</i>	Reserved for local use.																																																			
format	Log format.	option	-	default																																																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>Syslog format.</td></tr><tr><td><i>csv</i></td><td>CSV (Comma Separated Values) format.</td></tr><tr><td><i>cef</i></td><td>CEF (Common Event Format) format.</td></tr><tr><td><i>rfc5424</i></td><td>Syslog RFC5424 format.</td></tr></table>	Option	Description	<i>default</i>	Syslog format.	<i>csv</i>	CSV (Comma Separated Values) format.	<i>cef</i>	CEF (Common Event Format) format.	<i>rfc5424</i>	Syslog RFC5424 format.																																									
	Option	Description																																																		
	<i>default</i>	Syslog format.																																																		
	<i>csv</i>	CSV (Comma Separated Values) format.																																																		
	<i>cef</i>	CEF (Common Event Format) format.																																																		
<i>rfc5424</i>	Syslog RFC5424 format.																																																			

Parameter	Description	Type	Size	Default								
interface	Specify outgoing interface to reach server.	string	Maximum length: 15									
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>auto</td><td>Set outgoing interface automatically.</td></tr><tr><td>sdwan</td><td>Set outgoing interface by SD-WAN or policy routing rules.</td></tr><tr><td>specify</td><td>Set outgoing interface manually.</td></tr></table>				Option	Description	auto	Set outgoing interface automatically.	sdwan	Set outgoing interface by SD-WAN or policy routing rules.	specify	Set outgoing interface manually.
Option	Description											
auto	Set outgoing interface automatically.											
sdwan	Set outgoing interface by SD-WAN or policy routing rules.											
specify	Set outgoing interface manually.											
max-log-rate	Syslog maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0								
mode	Remote syslog logging over UDP/Reliable TCP.	option	-	udp								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>udp</td><td>Enable syslogging over UDP.</td></tr><tr><td>legacy-reliable</td><td>Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).</td></tr><tr><td>reliable</td><td>Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).</td></tr></table>				Option	Description	udp	Enable syslogging over UDP.	legacy-reliable	Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).	reliable	Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).
Option	Description											
udp	Enable syslogging over UDP.											
legacy-reliable	Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).											
reliable	Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).											
port	Server listen port.	integer	Minimum value: 0 Maximum value: 65535	514								
priority	Set log transmission priority.	option	-	default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>default</td><td>Set Syslog transmission priority to default.</td></tr><tr><td>low</td><td>Set Syslog transmission priority to low.</td></tr></table>				Option	Description	default	Set Syslog transmission priority to default.	low	Set Syslog transmission priority to low.		
Option	Description											
default	Set Syslog transmission priority to default.											
low	Set Syslog transmission priority to low.											
server	Address of remote syslog server.	string	Maximum length: 127									
source-ip	Source IP address of syslog.	string	Maximum length: 63									
ssl-min-protocol-version	Minimum supported protocol version for SSL/TLS connections.	option	-	default								



Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>default</i>	Follow system global setting.		
	<i>SSLv3</i>	SSLv3.		
	<i>TLSv1</i>	TLSv1.		
	<i>TLSv1-1</i>	TLSv1.1.		
	<i>TLSv1-2</i>	TLSv1.2.		
status	Enable/disable remote syslog logging.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Log to remote syslog server.		
	<i>disable</i>	Do not log to remote syslog server.		

### config custom-field-name

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 255	0
name	Field name.	string	Maximum length: 35	
custom	Field custom name.	string	Maximum length: 35	

### config log syslogd setting

Global settings for remote syslog server.

```
config log syslogd setting
    Description: Global settings for remote syslog server.
    set certificate {string}
    config custom-field-name
        Description: Custom field name for CEF format logging.
        edit <id>
            set name {string}
            set custom {string}
        next
    end
    set enc-algorithm [high-medium|high|...]
    set facility [kernel|user|...]
    set format [default|csv|...]
```

```

set interface {string}
set interface-select-method [auto|sdwan|...]
set max-log-rate {integer}
set mode [udp|legacy-reliable|...]
set port {integer}
set priority [default|low]
set server {string}
set source-ip {string}
set ssl-min-proto-version [default|SSLv3|...]
set status [enable|disable]
end

```

end

## config log syslogd setting

Parameter	Description	Type	Size	Default
certificate	Certificate used to communicate with Syslog server.	string	Maximum length: 35	
enc-algorithm	Enable/disable reliable syslogging with TLS encryption.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>high-medium</i>	SSL communication with high and medium encryption algorithms.		
	<i>high</i>	SSL communication with high encryption algorithms.		
	<i>low</i>	SSL communication with low encryption algorithms.		
	<i>disable</i>	Disable SSL communication.		
facility	Remote syslog facility.	option	-	local7
	<b>Option</b>	<b>Description</b>		
	<i>kernel</i>	Kernel messages.		
	<i>user</i>	Random user-level messages.		
	<i>mail</i>	Mail system.		
	<i>daemon</i>	System daemons.		
	<i>auth</i>	Security/authorization messages.		
	<i>syslog</i>	Messages generated internally by syslog.		
	<i>lpr</i>	Line printer subsystem.		
	<i>news</i>	Network news subsystem.		
	<i>uucp</i>	Network news subsystem.		
	<i>cron</i>	Clock daemon.		
	<i>authpriv</i>	Security/authorization messages (private).		
	<i>ftp</i>	FTP daemon.		

Parameter	Description	Type	Size	Default																										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ntp</i></td><td>NTP daemon.</td></tr><tr><td><i>audit</i></td><td>Log audit.</td></tr><tr><td><i>alert</i></td><td>Log alert.</td></tr><tr><td><i>clock</i></td><td>Clock daemon.</td></tr><tr><td><i>local0</i></td><td>Reserved for local use.</td></tr><tr><td><i>local1</i></td><td>Reserved for local use.</td></tr><tr><td><i>local2</i></td><td>Reserved for local use.</td></tr><tr><td><i>local3</i></td><td>Reserved for local use.</td></tr><tr><td><i>local4</i></td><td>Reserved for local use.</td></tr><tr><td><i>local5</i></td><td>Reserved for local use.</td></tr><tr><td><i>local6</i></td><td>Reserved for local use.</td></tr><tr><td><i>local7</i></td><td>Reserved for local use.</td></tr></table>	Option	Description	<i>ntp</i>	NTP daemon.	<i>audit</i>	Log audit.	<i>alert</i>	Log alert.	<i>clock</i>	Clock daemon.	<i>local0</i>	Reserved for local use.	<i>local1</i>	Reserved for local use.	<i>local2</i>	Reserved for local use.	<i>local3</i>	Reserved for local use.	<i>local4</i>	Reserved for local use.	<i>local5</i>	Reserved for local use.	<i>local6</i>	Reserved for local use.	<i>local7</i>	Reserved for local use.			
	Option	Description																												
	<i>ntp</i>	NTP daemon.																												
	<i>audit</i>	Log audit.																												
	<i>alert</i>	Log alert.																												
	<i>clock</i>	Clock daemon.																												
	<i>local0</i>	Reserved for local use.																												
	<i>local1</i>	Reserved for local use.																												
	<i>local2</i>	Reserved for local use.																												
	<i>local3</i>	Reserved for local use.																												
	<i>local4</i>	Reserved for local use.																												
	<i>local5</i>	Reserved for local use.																												
	<i>local6</i>	Reserved for local use.																												
<i>local7</i>	Reserved for local use.																													
format	Log format.	option	-	default																										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>Syslog format.</td></tr><tr><td><i>csv</i></td><td>CSV (Comma Separated Values) format.</td></tr><tr><td><i>cef</i></td><td>CEF (Common Event Format) format.</td></tr><tr><td><i>rfc5424</i></td><td>Syslog RFC5424 format.</td></tr></table>	Option	Description	<i>default</i>	Syslog format.	<i>csv</i>	CSV (Comma Separated Values) format.	<i>cef</i>	CEF (Common Event Format) format.	<i>rfc5424</i>	Syslog RFC5424 format.																			
	Option	Description																												
	<i>default</i>	Syslog format.																												
	<i>csv</i>	CSV (Comma Separated Values) format.																												
	<i>cef</i>	CEF (Common Event Format) format.																												
<i>rfc5424</i>	Syslog RFC5424 format.																													
interface	Specify outgoing interface to reach server.	string	Maximum length: 15																											
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto																										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto</i></td><td>Set outgoing interface automatically.</td></tr><tr><td><i>sdwan</i></td><td>Set outgoing interface by SD-WAN or policy routing rules.</td></tr><tr><td><i>specify</i></td><td>Set outgoing interface manually.</td></tr></table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.																					
	Option	Description																												
	<i>auto</i>	Set outgoing interface automatically.																												
	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.																												
<i>specify</i>	Set outgoing interface manually.																													

Parameter	Description	Type	Size	Default
max-log-rate	Syslog maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0
mode	Remote syslog logging over UDP/Reliable TCP.	option	-	udp
	<b>Option</b>	<b>Description</b>		
	<i>udp</i>	Enable syslogging over UDP.		
	<i>legacy-reliable</i>	Enable legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog).		
	<i>reliable</i>	Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).		
port	Server listen port.	integer	Minimum value: 0 Maximum value: 65535	514
priority	Set log transmission priority.	option	-	default
	<b>Option</b>	<b>Description</b>		
	<i>default</i>	Set Syslog transmission priority to default.		
	<i>low</i>	Set Syslog transmission priority to low.		
server	Address of remote syslog server.	string	Maximum length: 127	
source-ip	Source IP address of syslog.	string	Maximum length: 63	
ssl-min-protocol-version	Minimum supported protocol version for SSL/TLS connections.	option	-	default
	<b>Option</b>	<b>Description</b>		
	<i>default</i>	Follow system global setting.		
	<i>SSLv3</i>	SSLv3.		
	<i>TLSv1</i>	TLSv1.		
	<i>TLSv1-1</i>	TLSv1.1.		
	<i>TLSv1-2</i>	TLSv1.2.		
status	Enable/disable remote syslog logging.	option	-	disable

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Log to remote syslog server.		
	<i>disable</i>	Do not log to remote syslog server.		

### config custom-field-name

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 255	0
name	Field name.	string	Maximum length: 35	
custom	Field custom name.	string	Maximum length: 35	

### config log tacacs+accounting2 filter

Settings for TACACS+ accounting events filter.

```
config log tacacs+accounting2 filter
    Description: Settings for TACACS+ accounting events filter.
    set cli-cmd-audit [enable|disable]
    set config-change-audit [enable|disable]
    set login-audit [enable|disable]
end
```

### config log tacacs+accounting2 filter

Parameter	Description	Type	Size	Default
cli-cmd-audit	Enable/disable TACACS+ accounting for CLI commands audit.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable TACACS+ accounting for CLI commands audit.		
	<i>disable</i>	Disable TACACS+ accounting for CLI commands audit.		
config-change-audit	Enable/disable TACACS+ accounting for configuration change events audit.	option	-	enable

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable TACACS+ accounting for configuration change events audit.		
	<i>disable</i>	Disable TACACS+ accounting for configuration change events audit.		
login-audit	Enable/disable TACACS+ accounting for login events audit.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable TACACS+ accounting for login events audit.		
	<i>disable</i>	Disable TACACS+ accounting for login events audit.		

## config log tacacs+accounting2 setting

Settings for TACACS+ accounting.

```
config log tacacs+accounting2 setting
    Description: Settings for TACACS+ accounting.
    set server {string}
    set server-key {password}
    set status [enable|disable]
end
```

## config log tacacs+accounting2 setting

Parameter	Description	Type	Size	Default
server	Address of TACACS+ server.	string	Maximum length: 63	
server-key	Key to access the TACACS+ server.	password	Not Specified	
status	Enable/disable TACACS+ accounting.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable TACACS+ accounting.		
	<i>disable</i>	Disable TACACS+ accounting.		

## config log tacacs+accounting3 filter

Settings for TACACS+ accounting events filter.

```

config log tacacs+accounting3 filter
  Description: Settings for TACACS+ accounting events filter.
  set cli-cmd-audit [enable|disable]
  set config-change-audit [enable|disable]
  set login-audit [enable|disable]
end

```

## config log tacacs+accounting3 filter

Parameter	Description	Type	Size	Default						
cli-cmd-audit	Enable/disable TACACS+ accounting for CLI commands audit.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable TACACS+ accounting for CLI commands audit.</td></tr><tr><td><i>disable</i></td><td>Disable TACACS+ accounting for CLI commands audit.</td></tr></table>	Option	Description	<i>enable</i>	Enable TACACS+ accounting for CLI commands audit.	<i>disable</i>	Disable TACACS+ accounting for CLI commands audit.			
Option	Description									
<i>enable</i>	Enable TACACS+ accounting for CLI commands audit.									
<i>disable</i>	Disable TACACS+ accounting for CLI commands audit.									
config-change-audit	Enable/disable TACACS+ accounting for configuration change events audit.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable TACACS+ accounting for configuration change events audit.</td></tr><tr><td><i>disable</i></td><td>Disable TACACS+ accounting for configuration change events audit.</td></tr></table>	Option	Description	<i>enable</i>	Enable TACACS+ accounting for configuration change events audit.	<i>disable</i>	Disable TACACS+ accounting for configuration change events audit.			
Option	Description									
<i>enable</i>	Enable TACACS+ accounting for configuration change events audit.									
<i>disable</i>	Disable TACACS+ accounting for configuration change events audit.									
login-audit	Enable/disable TACACS+ accounting for login events audit.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable TACACS+ accounting for login events audit.</td></tr><tr><td><i>disable</i></td><td>Disable TACACS+ accounting for login events audit.</td></tr></table>	Option	Description	<i>enable</i>	Enable TACACS+ accounting for login events audit.	<i>disable</i>	Disable TACACS+ accounting for login events audit.			
Option	Description									
<i>enable</i>	Enable TACACS+ accounting for login events audit.									
<i>disable</i>	Disable TACACS+ accounting for login events audit.									

## config log tacacs+accounting3 setting

Settings for TACACS+ accounting.

```

config log tacacs+accounting3 setting
  Description: Settings for TACACS+ accounting.
  set server {string}
  set server-key {password}
  set status [enable|disable]
end

```

## config log tacacs+accounting3 setting

Parameter	Description	Type	Size	Default
server	Address of TACACS+ server.	string	Maximum length: 63	
server-key	Key to access the TACACS+ server.	password	Not Specified	
status	Enable/disable TACACS+ accounting.	option	-	disable
		Option	Description	
		<i>enable</i>	Enable TACACS+ accounting.	
		<i>disable</i>	Disable TACACS+ accounting.	

## config log tacacs+accounting filter

Settings for TACACS+ accounting events filter.

```
config log tacacs+accounting filter
  Description: Settings for TACACS+ accounting events filter.
  set cli-cmd-audit [enable|disable]
  set config-change-audit [enable|disable]
  set login-audit [enable|disable]
end
```

## config log tacacs+accounting filter

Parameter	Description	Type	Size	Default
cli-cmd-audit	Enable/disable TACACS+ accounting for CLI commands audit.	option	-	enable
		Option	Description	
		<i>enable</i>	Enable TACACS+ accounting for CLI commands audit.	
		<i>disable</i>	Disable TACACS+ accounting for CLI commands audit.	
config-change-audit	Enable/disable TACACS+ accounting for configuration change events audit.	option	-	enable
		Option	Description	
		<i>enable</i>	Enable TACACS+ accounting for configuration change events audit.	
		<i>disable</i>	Disable TACACS+ accounting for configuration change events audit.	



Parameter	Description	Type	Size	Default
login-audit	Enable/disable TACACS+ accounting for login events audit.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable TACACS+ accounting for login events audit.		
	<i>disable</i>	Disable TACACS+ accounting for login events audit.		

## config log tacacs+accounting setting

Settings for TACACS+ accounting.

```
config log tacacs+accounting setting
    Description: Settings for TACACS+ accounting.
    set server {string}
    set server-key {password}
    set status [enable|disable]
end
```

## config log tacacs+accounting setting

Parameter	Description	Type	Size	Default
server	Address of TACACS+ server.	string	Maximum length: 63	
server-key	Key to access the TACACS+ server.	password	Not Specified	
status	Enable/disable TACACS+ accounting.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable TACACS+ accounting.		
	<i>disable</i>	Disable TACACS+ accounting.		

## config log threat-weight

Configure threat weight settings.

```
config log threat-weight
    Description: Configure threat weight settings.
    config application
        Description: Application-control threat weight settings.
        edit <id>
            set category {integer}
            set level [disable|low|...]
        end
    end
```

```

        next
    end
    set blocked-connection [disable|low|...]
    set botnet-connection-detected [disable|low|...]
    set failed-connection [disable|low|...]
    config geolocation
        Description: Geolocation-based threat weight settings.
        edit <id>
            set country {string}
            set level [disable|low|...]
        next
    end
    config ips
        Description: IPS threat weight settings.
        set info-severity [disable|low|...]
        set low-severity [disable|low|...]
        set medium-severity [disable|low|...]
        set high-severity [disable|low|...]
        set critical-severity [disable|low|...]
    end
    config level
        Description: Score mapping for threat weight levels.
        set low {integer}
        set medium {integer}
        set high {integer}
        set critical {integer}
    end
    config malware
        Description: Anti-virus malware threat weight settings.
        set virus-infected [disable|low|...]
        set fortindr [disable|low|...]
        set file-blocked [disable|low|...]
        set command-blocked [disable|low|...]
        set oversized [disable|low|...]
        set virus-scan-error [disable|low|...]
        set switch-proto [disable|low|...]
        set mimefragmented [disable|low|...]
        set virus-file-type-executable [disable|low|...]
        set virus-outbreak-prevention [disable|low|...]
        set content-disarm [disable|low|...]
        set malware-list [disable|low|...]
        set ems-threat-feed [disable|low|...]
        set fsa-malicious [disable|low|...]
        set fsa-high-risk [disable|low|...]
        set fsa-medium-risk [disable|low|...]
    end
    set status [enable|disable]
    set url-block-detected [disable|low|...]
    config web
        Description: Web filtering threat weight settings.
        edit <id>
            set category {integer}
            set level [disable|low|...]
        next
    end
end
end

```

## config log threat-weight

Parameter	Description	Type	Size	Default												
blocked-connection	Threat weight score for blocked connections.	option	-	high												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable threat weight scoring for blocked connections.</td></tr><tr><td><i>low</i></td><td>Use the low level score for blocked connections.</td></tr><tr><td><i>medium</i></td><td>Use the medium level score for blocked connections.</td></tr><tr><td><i>high</i></td><td>Use the high level score for blocked connections.</td></tr><tr><td><i>critical</i></td><td>Use the critical level score for blocked connections.</td></tr></table>	Option	Description	<i>disable</i>	Disable threat weight scoring for blocked connections.	<i>low</i>	Use the low level score for blocked connections.	<i>medium</i>	Use the medium level score for blocked connections.	<i>high</i>	Use the high level score for blocked connections.	<i>critical</i>	Use the critical level score for blocked connections.			
Option	Description															
<i>disable</i>	Disable threat weight scoring for blocked connections.															
<i>low</i>	Use the low level score for blocked connections.															
<i>medium</i>	Use the medium level score for blocked connections.															
<i>high</i>	Use the high level score for blocked connections.															
<i>critical</i>	Use the critical level score for blocked connections.															
botnet-connection-detected	Threat weight score for detected botnet connections.	option	-	critical												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable threat weight scoring for detected botnet connections.</td></tr><tr><td><i>low</i></td><td>Use the low level score for detected botnet connections.</td></tr><tr><td><i>medium</i></td><td>Use the medium level score for detected botnet connections.</td></tr><tr><td><i>high</i></td><td>Use the high level score for detected botnet connections.</td></tr><tr><td><i>critical</i></td><td>Use the critical level score for detected botnet connections.</td></tr></table>	Option	Description	<i>disable</i>	Disable threat weight scoring for detected botnet connections.	<i>low</i>	Use the low level score for detected botnet connections.	<i>medium</i>	Use the medium level score for detected botnet connections.	<i>high</i>	Use the high level score for detected botnet connections.	<i>critical</i>	Use the critical level score for detected botnet connections.			
Option	Description															
<i>disable</i>	Disable threat weight scoring for detected botnet connections.															
<i>low</i>	Use the low level score for detected botnet connections.															
<i>medium</i>	Use the medium level score for detected botnet connections.															
<i>high</i>	Use the high level score for detected botnet connections.															
<i>critical</i>	Use the critical level score for detected botnet connections.															
failed-connection	Threat weight score for failed connections.	option	-	low												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable threat weight scoring for failed connections.</td></tr><tr><td><i>low</i></td><td>Use the low level score for failed connections.</td></tr><tr><td><i>medium</i></td><td>Use the medium level score for failed connections.</td></tr><tr><td><i>high</i></td><td>Use the high level score for failed connections.</td></tr><tr><td><i>critical</i></td><td>Use the critical level score for failed connections.</td></tr></table>	Option	Description	<i>disable</i>	Disable threat weight scoring for failed connections.	<i>low</i>	Use the low level score for failed connections.	<i>medium</i>	Use the medium level score for failed connections.	<i>high</i>	Use the high level score for failed connections.	<i>critical</i>	Use the critical level score for failed connections.			
Option	Description															
<i>disable</i>	Disable threat weight scoring for failed connections.															
<i>low</i>	Use the low level score for failed connections.															
<i>medium</i>	Use the medium level score for failed connections.															
<i>high</i>	Use the high level score for failed connections.															
<i>critical</i>	Use the critical level score for failed connections.															
status	Enable/disable the threat weight feature.	option	-	enable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable the threat weight feature.</td></tr><tr><td><i>disable</i></td><td>Disable the threat weight feature.</td></tr></table>	Option	Description	<i>enable</i>	Enable the threat weight feature.	<i>disable</i>	Disable the threat weight feature.									
Option	Description															
<i>enable</i>	Enable the threat weight feature.															
<i>disable</i>	Disable the threat weight feature.															

Parameter	Description	Type	Size	Default
url-block-detected	Threat weight score for URL blocking.	option	-	high
	Option	Description		
	<i>disable</i>	Disable threat weight scoring for URL blocking.		
	<i>low</i>	Use the low level score for URL blocking.		
	<i>medium</i>	Use the medium level score for URL blocking.		
	<i>high</i>	Use the high level score for URL blocking.		
	<i>critical</i>	Use the critical level score for URL blocking.		

## config application

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 255	0
category	Application category.	integer	Minimum value: 0 Maximum value: 65535	0
level	Threat weight score for Application events.	option	-	low
	Option	Description		
	<i>disable</i>	Disable threat weight scoring for Application events.		
	<i>low</i>	Use the low level score for Application events.		
	<i>medium</i>	Use the medium level score for Application events.		
	<i>high</i>	Use the high level score for Application events.		
	<i>critical</i>	Use the critical level score for Application events.		

## config geolocation

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 255	0

Parameter	Description	Type	Size	Default												
country	Country code.	string	Maximum length: 2													
level	Threat weight score for Geolocation-based events.	option	-	low												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable threat weight scoring for Geolocation-based events.</td></tr><tr><td><i>low</i></td><td>Use the low level score for Geolocation-based events.</td></tr><tr><td><i>medium</i></td><td>Use the medium level score for Geolocation-based events.</td></tr><tr><td><i>high</i></td><td>Use the high level score for Geolocation-based events.</td></tr><tr><td><i>critical</i></td><td>Use the critical level score for Geolocation-based events.</td></tr></table>				Option	Description	<i>disable</i>	Disable threat weight scoring for Geolocation-based events.	<i>low</i>	Use the low level score for Geolocation-based events.	<i>medium</i>	Use the medium level score for Geolocation-based events.	<i>high</i>	Use the high level score for Geolocation-based events.	<i>critical</i>	Use the critical level score for Geolocation-based events.
	Option	Description														
	<i>disable</i>	Disable threat weight scoring for Geolocation-based events.														
	<i>low</i>	Use the low level score for Geolocation-based events.														
	<i>medium</i>	Use the medium level score for Geolocation-based events.														
	<i>high</i>	Use the high level score for Geolocation-based events.														
<i>critical</i>	Use the critical level score for Geolocation-based events.															

## config ips

Parameter	Description	Type	Size	Default												
info-severity	Threat weight score for IPS info severity events.	option	-	disable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable threat weight scoring for IPS info severity events.</td></tr><tr><td>low</td><td>Use the low level score for IPS info severity events.</td></tr><tr><td>medium</td><td>Use the medium level score for IPS info severity events.</td></tr><tr><td>high</td><td>Use the high level score for IPS info severity events.</td></tr><tr><td>critical</td><td>Use the critical level score for IPS info severity events.</td></tr></table>	Option	Description	disable	Disable threat weight scoring for IPS info severity events.	low	Use the low level score for IPS info severity events.	medium	Use the medium level score for IPS info severity events.	high	Use the high level score for IPS info severity events.	critical	Use the critical level score for IPS info severity events.			
	Option	Description														
	disable	Disable threat weight scoring for IPS info severity events.														
	low	Use the low level score for IPS info severity events.														
	medium	Use the medium level score for IPS info severity events.														
	high	Use the high level score for IPS info severity events.														
critical	Use the critical level score for IPS info severity events.															
low-severity	Threat weight score for IPS low severity events.	option	-	low												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable threat weight scoring for IPS low severity events.</td></tr><tr><td>low</td><td>Use the low level score for IPS low severity events.</td></tr><tr><td>medium</td><td>Use the medium level score for IPS low severity events.</td></tr><tr><td>high</td><td>Use the high level score for IPS low severity events.</td></tr><tr><td>critical</td><td>Use the critical level score for IPS low severity events.</td></tr></table>	Option	Description	disable	Disable threat weight scoring for IPS low severity events.	low	Use the low level score for IPS low severity events.	medium	Use the medium level score for IPS low severity events.	high	Use the high level score for IPS low severity events.	critical	Use the critical level score for IPS low severity events.			
	Option	Description														
	disable	Disable threat weight scoring for IPS low severity events.														
	low	Use the low level score for IPS low severity events.														
	medium	Use the medium level score for IPS low severity events.														
	high	Use the high level score for IPS low severity events.														
critical	Use the critical level score for IPS low severity events.															
medium-severity	Threat weight score for IPS medium severity events.	option	-	medium												

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable threat weight scoring for IPS medium severity events.		
	<i>low</i>	Use the low level score for IPS medium severity events.		
	<i>medium</i>	Use the medium level score for IPS medium severity events.		
	<i>high</i>	Use the high level score for IPS medium severity events.		
	<i>critical</i>	Use the critical level score for IPS medium severity events.		
high-severity	Threat weight score for IPS high severity events.	option	-	high
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable threat weight scoring for IPS high severity events.		
	<i>low</i>	Use the low level score for IPS high severity events.		
	<i>medium</i>	Use the medium level score for IPS high severity events.		
	<i>high</i>	Use the high level score for IPS high severity events.		
	<i>critical</i>	Use the critical level score for IPS high severity events.		
critical-severity	Threat weight score for IPS critical severity events.	option	-	critical
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable threat weight scoring for IPS critical severity events.		
	<i>low</i>	Use the low level score for IPS critical severity events.		
	<i>medium</i>	Use the medium level score for IPS critical severity events.		
	<i>high</i>	Use the high level score for IPS critical severity events.		
	<i>critical</i>	Use the critical level score for IPS critical severity events.		

## config level

Parameter	Description	Type	Size	Default
low	Low level score value.	integer	Minimum value: 1 Maximum value: 100	5
medium	Medium level score value.	integer	Minimum value: 1 Maximum value: 100	10

Parameter	Description	Type	Size	Default
high	High level score value.	integer	Minimum value: 1 Maximum value: 100	30
critical	Critical level score value.	integer	Minimum value: 1 Maximum value: 100	50

## config malware

Parameter	Description	Type	Size	Default
virus-infected	Threat weight score for virus (infected) detected.	option	-	critical
	Option	Description		
	disable	Disable threat weight scoring for virus (infected) detected.		
	low	Use the low level score for virus (infected) detected.		
	medium	Use the medium level score for virus (infected) detected.		
	high	Use the high level score for virus (infected) detected.		
	critical	Use the critical level score for virus (infected) detected.		
fortindr	Threat weight score for FortiNDR-detected virus.	option	-	critical
	Option	Description		
	disable	Disable threat weight scoring for virus detected by FortiNDR.		
	low	Use the low level score for virus detected by FortiNDR.		
	medium	Use the medium level score for virus detected by FortiNDR.		
	high	Use the high level score for virus detected by FortiNDR.		
	critical	Use the critical level score for virus detected by FortiNDR.		
file-blocked	Threat weight score for blocked file detected.	option	-	low
	Option	Description		
	disable	Disable threat weight scoring for blocked file detected.		
	low	Use the low level score for blocked file detected.		
	medium	Use the medium level score for blocked file detected.		
	high	Use the high level score for blocked file detected.		
	critical	Use the critical level score for blocked file detected.		

Parameter	Description	Type	Size	Default
command-blocked	Threat weight score for blocked command detected.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable threat weight scoring for blocked command detected.		
	<i>low</i>	Use the low level score for blocked command detected.		
	<i>medium</i>	Use the medium level score for blocked command detected.		
	<i>high</i>	Use the high level score for blocked command detected.		
	<i>critical</i>	Use the critical level score for blocked command detected.		
oversized	Threat weight score for oversized file detected.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable threat weight scoring for oversized file detected.		
	<i>low</i>	Use the low level score for oversized file detected.		
	<i>medium</i>	Use the medium level score for oversized file detected.		
	<i>high</i>	Use the high level score for oversized file detected.		
	<i>critical</i>	Use the critical level score for oversized file detected.		
virus-scan-error	Threat weight score for virus (scan error) detected.	option	-	high
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable threat weight scoring for virus (scan error) detected.		
	<i>low</i>	Use the low level score for virus (scan error) detected.		
	<i>medium</i>	Use the medium level score for virus (scan error) detected.		
	<i>high</i>	Use the high level score for virus (scan error) detected.		
	<i>critical</i>	Use the critical level score for virus (scan error) detected.		
switch-proto	Threat weight score for switch proto detected.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable threat weight scoring for switch proto detected.		
	<i>low</i>	Use the low level score for switch proto detected.		
	<i>medium</i>	Use the medium level score for switch proto detected.		
	<i>high</i>	Use the high level score for switch proto detected.		
	<i>critical</i>	Use the critical level score for switch proto detected.		
mimefragmented	Threat weight score for mimefragmented detected.	option	-	disable



Parameter	Description	Type	Size	Default												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable threat weight scoring for mimefragmented detected.</td></tr><tr><td><i>low</i></td><td>Use the low level score for mimefragmented detected.</td></tr><tr><td><i>medium</i></td><td>Use the medium level score for mimefragmented detected.</td></tr><tr><td><i>high</i></td><td>Use the high level score for mimefragmented detected.</td></tr><tr><td><i>critical</i></td><td>Use the critical level score for mimefragmented detected.</td></tr></table>	Option	Description	<i>disable</i>	Disable threat weight scoring for mimefragmented detected.	<i>low</i>	Use the low level score for mimefragmented detected.	<i>medium</i>	Use the medium level score for mimefragmented detected.	<i>high</i>	Use the high level score for mimefragmented detected.	<i>critical</i>	Use the critical level score for mimefragmented detected.			
	Option	Description														
	<i>disable</i>	Disable threat weight scoring for mimefragmented detected.														
	<i>low</i>	Use the low level score for mimefragmented detected.														
	<i>medium</i>	Use the medium level score for mimefragmented detected.														
	<i>high</i>	Use the high level score for mimefragmented detected.														
	<i>critical</i>	Use the critical level score for mimefragmented detected.														
virus-file-type-executable	Threat weight score for virus (file type executable) detected.	option	-	medium												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable threat weight scoring for virus (filetype executable) detected.</td></tr><tr><td><i>low</i></td><td>Use the low level score for virus (filetype executable) detected.</td></tr><tr><td><i>medium</i></td><td>Use the medium level score for virus (filetype executable) detected.</td></tr><tr><td><i>high</i></td><td>Use the high level score for virus (filetype executable) detected.</td></tr><tr><td><i>critical</i></td><td>Use the critical level score for virus (filetype executable) detected.</td></tr></table>	Option	Description	<i>disable</i>	Disable threat weight scoring for virus (filetype executable) detected.	<i>low</i>	Use the low level score for virus (filetype executable) detected.	<i>medium</i>	Use the medium level score for virus (filetype executable) detected.	<i>high</i>	Use the high level score for virus (filetype executable) detected.	<i>critical</i>	Use the critical level score for virus (filetype executable) detected.			
	Option	Description														
	<i>disable</i>	Disable threat weight scoring for virus (filetype executable) detected.														
	<i>low</i>	Use the low level score for virus (filetype executable) detected.														
	<i>medium</i>	Use the medium level score for virus (filetype executable) detected.														
	<i>high</i>	Use the high level score for virus (filetype executable) detected.														
	<i>critical</i>	Use the critical level score for virus (filetype executable) detected.														
virus-outbreak-prevention	Threat weight score for virus (outbreak prevention) event.	option	-	critical												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable threat weight scoring for virus (outbreak prevention) event.</td></tr><tr><td><i>low</i></td><td>Use the low level score for virus (outbreak prevention) event.</td></tr><tr><td><i>medium</i></td><td>Use the medium level score for virus (outbreak prevention) event.</td></tr><tr><td><i>high</i></td><td>Use the high level score for virus (outbreak prevention) event.</td></tr><tr><td><i>critical</i></td><td>Use the critical level score for virus (outbreak prevention) event.</td></tr></table>	Option	Description	<i>disable</i>	Disable threat weight scoring for virus (outbreak prevention) event.	<i>low</i>	Use the low level score for virus (outbreak prevention) event.	<i>medium</i>	Use the medium level score for virus (outbreak prevention) event.	<i>high</i>	Use the high level score for virus (outbreak prevention) event.	<i>critical</i>	Use the critical level score for virus (outbreak prevention) event.			
	Option	Description														
	<i>disable</i>	Disable threat weight scoring for virus (outbreak prevention) event.														
	<i>low</i>	Use the low level score for virus (outbreak prevention) event.														
	<i>medium</i>	Use the medium level score for virus (outbreak prevention) event.														
	<i>high</i>	Use the high level score for virus (outbreak prevention) event.														
	<i>critical</i>	Use the critical level score for virus (outbreak prevention) event.														
content-disarm	Threat weight score for virus (content disarm) detected.	option	-	medium												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable threat weight scoring for virus (content disarm) detected.</td></tr><tr><td><i>low</i></td><td>Use the low level score for virus (content disarm) detected.</td></tr><tr><td><i>medium</i></td><td>Use the medium level score for virus (content disarm) detected.</td></tr><tr><td><i>high</i></td><td>Use the high level score for virus (content disarm) detected.</td></tr><tr><td><i>critical</i></td><td>Use the critical level score for virus (content disarm) detected.</td></tr></table>	Option	Description	<i>disable</i>	Disable threat weight scoring for virus (content disarm) detected.	<i>low</i>	Use the low level score for virus (content disarm) detected.	<i>medium</i>	Use the medium level score for virus (content disarm) detected.	<i>high</i>	Use the high level score for virus (content disarm) detected.	<i>critical</i>	Use the critical level score for virus (content disarm) detected.			
	Option	Description														
	<i>disable</i>	Disable threat weight scoring for virus (content disarm) detected.														
	<i>low</i>	Use the low level score for virus (content disarm) detected.														
	<i>medium</i>	Use the medium level score for virus (content disarm) detected.														
	<i>high</i>	Use the high level score for virus (content disarm) detected.														
	<i>critical</i>	Use the critical level score for virus (content disarm) detected.														

Parameter	Description	Type	Size	Default												
malware-list	Threat weight score for virus (malware list) detected.	option	-	medium												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable threat weight scoring for virus (malware list) detected.</td></tr><tr><td><i>low</i></td><td>Use the low level score for virus (malware list) detected.</td></tr><tr><td><i>medium</i></td><td>Use the medium level score for virus (malware list) detected.</td></tr><tr><td><i>high</i></td><td>Use the high level score for virus (malware list) detected.</td></tr><tr><td><i>critical</i></td><td>Use the critical level score for virus (malware list) detected.</td></tr></table>	Option	Description	<i>disable</i>	Disable threat weight scoring for virus (malware list) detected.	<i>low</i>	Use the low level score for virus (malware list) detected.	<i>medium</i>	Use the medium level score for virus (malware list) detected.	<i>high</i>	Use the high level score for virus (malware list) detected.	<i>critical</i>	Use the critical level score for virus (malware list) detected.			
Option	Description															
<i>disable</i>	Disable threat weight scoring for virus (malware list) detected.															
<i>low</i>	Use the low level score for virus (malware list) detected.															
<i>medium</i>	Use the medium level score for virus (malware list) detected.															
<i>high</i>	Use the high level score for virus (malware list) detected.															
<i>critical</i>	Use the critical level score for virus (malware list) detected.															
ems-threat-feed	Threat weight score for virus (EMS threat feed) detected.	option	-	medium												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable threat weight scoring for virus (EMS threat feed) detected.</td></tr><tr><td><i>low</i></td><td>Use the low level score for virus (EMS threat feed) detected.</td></tr><tr><td><i>medium</i></td><td>Use the medium level score for virus (EMS threat feed) detected.</td></tr><tr><td><i>high</i></td><td>Use the high level score for virus (EMS threat feed) detected.</td></tr><tr><td><i>critical</i></td><td>Use the critical level score for virus (EMS threat feed) detected.</td></tr></table>	Option	Description	<i>disable</i>	Disable threat weight scoring for virus (EMS threat feed) detected.	<i>low</i>	Use the low level score for virus (EMS threat feed) detected.	<i>medium</i>	Use the medium level score for virus (EMS threat feed) detected.	<i>high</i>	Use the high level score for virus (EMS threat feed) detected.	<i>critical</i>	Use the critical level score for virus (EMS threat feed) detected.			
Option	Description															
<i>disable</i>	Disable threat weight scoring for virus (EMS threat feed) detected.															
<i>low</i>	Use the low level score for virus (EMS threat feed) detected.															
<i>medium</i>	Use the medium level score for virus (EMS threat feed) detected.															
<i>high</i>	Use the high level score for virus (EMS threat feed) detected.															
<i>critical</i>	Use the critical level score for virus (EMS threat feed) detected.															
fsa-malicious	Threat weight score for FortiSandbox malicious malware detected.	option	-	critical												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable threat weight scoring for FortiSandbox malicious malware detected.</td></tr><tr><td><i>low</i></td><td>Use the low level score for FortiSandbox malicious malware detected.</td></tr><tr><td><i>medium</i></td><td>Use the medium level score for FortiSandbox malicious malware detected.</td></tr><tr><td><i>high</i></td><td>Use the high level score for FortiSandbox malicious malware detected.</td></tr><tr><td><i>critical</i></td><td>Use the critical level score for FortiSandbox malicious malware detected.</td></tr></table>	Option	Description	<i>disable</i>	Disable threat weight scoring for FortiSandbox malicious malware detected.	<i>low</i>	Use the low level score for FortiSandbox malicious malware detected.	<i>medium</i>	Use the medium level score for FortiSandbox malicious malware detected.	<i>high</i>	Use the high level score for FortiSandbox malicious malware detected.	<i>critical</i>	Use the critical level score for FortiSandbox malicious malware detected.			
Option	Description															
<i>disable</i>	Disable threat weight scoring for FortiSandbox malicious malware detected.															
<i>low</i>	Use the low level score for FortiSandbox malicious malware detected.															
<i>medium</i>	Use the medium level score for FortiSandbox malicious malware detected.															
<i>high</i>	Use the high level score for FortiSandbox malicious malware detected.															
<i>critical</i>	Use the critical level score for FortiSandbox malicious malware detected.															
fsa-high-risk	Threat weight score for FortiSandbox high risk malware detected.	option	-	high												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable threat weight scoring for FortiSandbox high risk malware detected.</td></tr></table>	Option	Description	<i>disable</i>	Disable threat weight scoring for FortiSandbox high risk malware detected.											
Option	Description															
<i>disable</i>	Disable threat weight scoring for FortiSandbox high risk malware detected.															

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>low</i>	Use the low level score for FortiSandbox high risk malware detected.		
	<i>medium</i>	Use the medium level score for FortiSandbox high risk malware detected.		
	<i>high</i>	Use the high level score for FortiSandbox high risk malware detected.		
	<i>critical</i>	Use the critical level score for FortiSandbox high risk malware detected.		
fsa-medium-risk	Threat weight score for FortiSandbox medium risk malware detected.	option	-	medium
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable threat weight scoring for FortiSandbox medium risk malware detected.		
	<i>low</i>	Use the low level score for FortiSandbox medium risk malware detected.		
	<i>medium</i>	Use the medium level score for FortiSandbox medium risk malware detected.		
	<i>high</i>	Use the high level score for FortiSandbox medium risk malware detected.		
	<i>critical</i>	Use the critical level score for FortiSandbox medium risk malware detected.		

## config web

Parameter	Description	Type	Size	Default												
id	Entry ID.	integer	Minimum value: 0 Maximum value: 255	0												
category	Threat weight score for web category filtering matches.	integer	Minimum value: 0 Maximum value: 255	0												
level	Threat weight score for web category filtering matches.	option	-	low												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable threat weight scoring for web category filtering matches.</td></tr><tr><td><i>low</i></td><td>Use the low level score for web category filtering matches.</td></tr><tr><td><i>medium</i></td><td>Use the medium level score for web category filtering matches.</td></tr><tr><td><i>high</i></td><td>Use the high level score for web category filtering matches.</td></tr><tr><td><i>critical</i></td><td>Use the critical level score for web category filtering matches.</td></tr></table>				Option	Description	<i>disable</i>	Disable threat weight scoring for web category filtering matches.	<i>low</i>	Use the low level score for web category filtering matches.	<i>medium</i>	Use the medium level score for web category filtering matches.	<i>high</i>	Use the high level score for web category filtering matches.	<i>critical</i>	Use the critical level score for web category filtering matches.
Option	Description															
<i>disable</i>	Disable threat weight scoring for web category filtering matches.															
<i>low</i>	Use the low level score for web category filtering matches.															
<i>medium</i>	Use the medium level score for web category filtering matches.															
<i>high</i>	Use the high level score for web category filtering matches.															
<i>critical</i>	Use the critical level score for web category filtering matches.															

## config log webtrends filter

Filters for WebTrends.

```
config log webtrends filter
  Description: Filters for WebTrends.
  set anomaly [enable|disable]
  set forward-traffic [enable|disable]
  config free-style
    Description: Free style filters.
    edit <id>
      set category [traffic|event|...]
      set filter {string}
      set filter-type [include|exclude]
    next
  end
  set gtp [enable|disable]
  set local-traffic [enable|disable]
  set multicast-traffic [enable|disable]
  set severity [emergency|alert|...]
  set sniffer-traffic [enable|disable]
  set voip [enable|disable]
  set ztna-traffic [enable|disable]
end
```

## config log webtrends filter

Parameter	Description	Type	Size	Default
anomaly	Enable/disable anomaly logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable anomaly logging.		
	<i>disable</i>	Disable anomaly logging.		
forward-traffic	Enable/disable forward traffic logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable forward traffic logging.		
	<i>disable</i>	Disable forward traffic logging.		
gtp *	Enable/disable GTP messages logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable GTP messages logging.		
	<i>disable</i>	Disable GTP messages logging.		
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable local in or out traffic logging.		
	<i>disable</i>	Disable local in or out traffic logging.		
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable multicast traffic logging.		
	<i>disable</i>	Disable multicast traffic logging.		
severity	Lowest severity level to log to WebTrends.	option	-	information
	<b>Option</b>	<b>Description</b>		
	<i>emergency</i>	Emergency level.		
	<i>alert</i>	Alert level.		
	<i>critical</i>	Critical level.		
	<i>error</i>	Error level.		
	<i>warning</i>	Warning level.		
	<i>notification</i>	Notification level.		
	<i>information</i>	Information level.		
	<i>debug</i>	Debug level.		
sniffer-traffic	Enable/disable sniffer traffic logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable sniffer traffic logging.		
	<i>disable</i>	Disable sniffer traffic logging.		
voip	Enable/disable VoIP logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable VoIP logging.		
	<i>disable</i>	Disable VoIP logging.		
ztna-traffic	Enable/disable ztna traffic logging.	option	-	enable

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable ztna traffic logging.		
	<i>disable</i>	Disable ztna traffic logging.		

\* This parameter may not exist in some models.

### config free-style

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
category	Log category.	option	-	traffic
	<b>Option</b>	<b>Description</b>		
	<i>traffic</i>	Traffic log.		
	<i>event</i>	Event log.		
	<i>virus</i>	Antivirus log.		
	<i>webfilter</i>	Web filter log.		
	<i>attack</i>	Attack log.		
	<i>spam</i>	Antispam log.		
	<i>anomaly</i>	Anomaly log.		
	<i>voip</i>	VoIP log.		
	<i>dlp</i>	DLP log.		
	<i>app-ctrl</i>	Application control log.		
	<i>waf</i>	Web application firewall log.		
	<i>dns</i>	DNS detail log.		
	<i>ssh</i>	SSH log.		
	<i>ssl</i>	SSL log.		
	<i>file-filter</i>	File filter log.		
	<i>icap</i>	ICAP log.		

Parameter	Description	Type	Size	Default						
filter	Free style filter string.	string	Maximum length: 1023							
filter-type	Include/exclude logs that match the filter.	option	-	include						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>include</i></td><td>Include logs that match the filter.</td></tr><tr><td><i>exclude</i></td><td>Exclude logs that match the filter.</td></tr></table>	Option	Description	<i>include</i>	Include logs that match the filter.	<i>exclude</i>	Exclude logs that match the filter.			
Option	Description									
<i>include</i>	Include logs that match the filter.									
<i>exclude</i>	Exclude logs that match the filter.									

## config log webtrends setting

Settings for WebTrends.

```
config log webtrends setting
    Description: Settings for WebTrends.
    set server {string}
    set status [enable|disable]
end
```

## config log webtrends setting

Parameter	Description	Type	Size	Default						
server	Address of the remote WebTrends server.	string	Maximum length: 63							
status	Enable/disable logging to WebTrends.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable logging to WebTrends.</td></tr><tr><td><i>disable</i></td><td>Disble logging to WebTrends.</td></tr></table>				Option	Description	<i>enable</i>	Enable logging to WebTrends.	<i>disable</i>	Disble logging to WebTrends.
Option	Description									
<i>enable</i>	Enable logging to WebTrends.									
<i>disable</i>	Disble logging to WebTrends.									

## monitoring

This section includes syntax for the following commands:

- [config monitoring np6-ipsec-engine on page 732](#)
- [config monitoring npu-hpe on page 733](#)

### config monitoring np6-ipsec-engine



This command is available for model(s): FortiGate 1000D, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 1500DT, FortiGate 1500D, FortiGate 2000E, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 3000D, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 401E, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 601E, FortiGate 800D, FortiGate 900D.

It is not available for: FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 140E-POE, FortiGate 140E, FortiGate 1800F, FortiGate 1801F, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2600F, FortiGate 2601F, FortiGate 3000F, FortiGate 3001F, FortiGate 3500F, FortiGate 3501F, FortiGate 400F, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 600F, FortiGate 601F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 90E, FortiGate 91E, FortiGate VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

Configure NP6 IPsec engine status monitoring.

```
config monitoring np6-ipsec-engine
    Description: Configure NP6 IPsec engine status monitoring.
    set interval {integer}
    set status [enable|disable]
    set threshold {user}
end
```



## config monitoring np6-ipsec-engine

Parameter	Description	Type	Size	Default
interval	IPsec engine status check interval.	integer	Minimum value: 1 Maximum value: 60	1
status	Enable/disable NP6 IPsec engine status monitoring.	option	-	disable
	Option	Description		
	enable	Enable setting.		
	disable	Disable setting.		
threshold	IPsec engine status check threshold. Example: Log is generated if IPsec engine 0 is busy each of every 15 consecutive interval checks.	user	Not Specified	

## config monitoring npu-hpe



This command is available for model(s): FortiGate 1000D, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 1500DT, FortiGate 1500D, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 800D, FortiGate 900D.

It is not available for: FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 140E-POE, FortiGate 140E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 90E, FortiGate 91E, FortiGate VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

Configure npu-hpe status monitoring.

```
config monitoring npu-hpe
    Description: Configure npu-hpe status monitoring.
```

```

set interval {integer}
set multipliers {user}
set status [enable|disable]
end

```

## config monitoring npu-hpe

Parameter	Description	Type	Size	Default
interval	HPE status check interval.	integer	Minimum value: 1 Maximum value: 60	1
multipliers	HPE type interval multipliers. An event log is generated after every (interval * multiplier)seconds as configured for any HPE type when drops occur for that HPE type. An attack log is generated after every (4 * multiplier) number of continuous event logs.	user	Not Specified	
status	Enable/disable HPE status monitoring.	option	-	disable
		Option	Description	
		<i>enable</i>	Enable setting.	
		<i>disable</i>	Disable setting.	

## nsxt

This section includes syntax for the following commands:

- [config nsxt service-chain on page 735](#)
- [config nsxt setting on page 737](#)

### config nsxt service-chain



This command is available for model(s): FortiGate VM64.

It is not available for: FortiGate 1000D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

Configure NSX-T service chain.

```
config nsxt service-chain
  Description: Configure NSX-T service chain.
  edit <id>
    set name {string}
    config service-index
      Description: Configure service index.
      edit <id>
        set reverse-index {integer}
        set name {string}
        set vd {string}
      next
    end
```

---

```
    next
end
```

### config nsxt service-chain

Parameter	Description	Type	Size	Default
id	Chain ID.	integer	Minimum value: 0 Maximum value: 1023	0
name	Chain name.	string	Maximum length: 63	

### config service-index

Parameter	Description	Type	Size	Default
id	Service index.	integer	Minimum value: 0 Maximum value: 255	0
reverse-index	Reverse service index.	integer	Minimum value: 1 Maximum value: 255	1
name	Index name.	string	Maximum length: 63	
vd	VDOM name.	string	Maximum length: 31	

## config nsxt setting



This command is available for model(s): FortiGate VM64.

It is not available for: FortiGate 1000D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

Configure NSX-T setting.

```
config nsxt setting
    Description: Configure NSX-T setting.
    set liveness [enable|disable]
    set service {string}
end
```

## config nsxt setting

Parameter	Description	Type	Size	Default
liveness	Enable/disable liveness detection packet forwarding.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable liveness detection packet forwarding.		
	<i>disable</i>	Disable liveness detection packet forwarding.		
service	Service name.	string	Maximum length: 63	

This section includes syntax for the following commands:

- [config pfcp message-filter on page 738](#)

## config pfcp message-filter



This command is available for model(s): FortiGate 2600F, FortiGate 3000F, FortiGate 3001F, FortiGate 3400E.

It is not available for: FortiGate 1000D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2601F, FortiGate 3000D, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

Message filter for PFCP messages.

```
config pfcp message-filter
  Description: Message filter for PFCP messages.
  edit <name>
    set association-release [allow|deny]
    set association-setup [allow|deny]
    set association-update [allow|deny]
    set heartbeat [allow|deny]
    set node-report [allow|deny]
    set pfd-management [allow|deny]
    set session-deletion [allow|deny]
    set session-establish [allow|deny]
    set session-modification [allow|deny]
    set session-report [allow|deny]
    set session-set-deletion [allow|deny]
```

```

set unknown-message [allow|deny]
set unknown-message-allow-list <id1>, <id2>, ...
set version-not-support [allow|deny]
next
end

```

## config pfcp message-filter

Parameter	Description	Type	Size	Default
association-release	Allow or deny PFCP association release request (9) and PFCP association release response (10).	option	-	allow
	<b>Option</b>		<b>Description</b>	
	<i>allow</i>		Allow message.	
	<i>deny</i>		Deny message.	
association-setup	Allow or deny PFCP association setup request (5) and PFCP association setup response (6).	option	-	allow
	<b>Option</b>		<b>Description</b>	
	<i>allow</i>		Allow message.	
	<i>deny</i>		Deny message.	
association-update	Allow or deny PFCP association update request (7) and PFCP association update response (8).	option	-	allow
	<b>Option</b>		<b>Description</b>	
	<i>allow</i>		Allow message.	
	<i>deny</i>		Deny message.	
heartbeat	Allow or deny PFCP heartbeat request (1) and PFCP heartbeat response (2).	option	-	allow
	<b>Option</b>		<b>Description</b>	
	<i>allow</i>		Allow message.	
	<i>deny</i>		Deny message.	
name	Message filter name.	string	Maximum length: 63	
node-report	Allow or deny PFCP node report request (12) and PFCP node report response (13).	option	-	allow

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow message.		
	<i>deny</i>	Deny message.		
pfid-management	Allow or deny PFCP PFD management request (3) and PFCP PFD management response (4).	option	-	allow
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow message.		
	<i>deny</i>	Deny message.		
session-deletion	Allow or deny PFCP session deletion request (54) and PFCP session deletion response (55).	option	-	allow
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow message.		
	<i>deny</i>	Deny message.		
session-establish	Allow or deny PFCP session establishment request (50) and PFCP session establishment response (51).	option	-	allow
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow message.		
	<i>deny</i>	Deny message.		
session-modification	Allow or deny PFCP session modification request (52) and PFCP session modification response (53).	option	-	allow
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow message.		
	<i>deny</i>	Deny message.		
session-report	Allow or deny PFCP session report request (56) and PFCP session report response (57).	option	-	allow
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow message.		
	<i>deny</i>	Deny message.		
session-set-deletion	Allow or deny PFCP session set deletion request (14) and PFCP session set deletion response (15).	option	-	allow



Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow message.		
	<i>deny</i>	Deny message.		
unknown-message	Allow or deny unknown messages.	option	-	allow
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow setting.		
	<i>deny</i>	Deny setting.		
unknown-message-allow-list <id>	Allow list of unknown messages. Message IDs (range from 1 to 255).	integer	Minimum value: 1 Maximum value: 255	
version-not-support	Allow or deny PFCP version not supported response (11).	option	-	allow
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow message.		
	<i>deny</i>	Deny message.		

# report

This section includes syntax for the following commands:

- [config report layout on page 742](#)
- [config report setting on page 751](#)

## config report layout



This command is available for model(s): FortiGate 1000D, FortiGate 101E, FortiGate 101F, FortiGate 1101E, FortiGate 1200D, FortiGate 1500DT, FortiGate 1500D, FortiGate 1801F, FortiGate 2000E, FortiGate 201E, FortiGate 201F, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3001F, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3301E, FortiGate 3401E, FortiGate 3501F, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 401E, FortiGate 401F, FortiGate 4201F, FortiGate 4401F, FortiGate 5001E1, FortiGate 501E, FortiGate 601E, FortiGate 601F, FortiGate 61E, FortiGate 61F, FortiGate 71F, FortiGate 800D, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 91E, FortiGate VM64, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 1100E, FortiGate 140E-POE, FortiGate 140E, FortiGate 1800F, FortiGate 200E, FortiGate 200F, FortiGate 2200E, FortiGate 3000F, FortiGate 300E, FortiGate 3300E, FortiGate 3400E, FortiGate 3500F, FortiGate 3600E, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4400F, FortiGate 5001E, FortiGate 500E, FortiGate 600E, FortiGate 600F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 70F, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 90E, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 80F 2R.

Report layout configuration.

```
config report layout
  Description: Report layout configuration.
  edit <name>
    config body-item
      Description: Configure report body item.
      edit <id>
        set description {string}
        set type [text|image|...]
        set style {string}
        set top-n {integer}
        config parameters
          Description: Parameters.
          edit <id>
```

```

        set name {string}
        set value {string}
    next
end
set text-component [text|heading1|...]
set content {string}
set img-src {string}
set chart {string}
set chart-options {option1}, {option2}, ...
set misc-component [hline|page-break|...]
set title {string}
next
end
set cutoff-option [run-time|custom]
set cutoff-time {user}
set day [sunday|monday|...]
set description {string}
set email-recipients {string}
set email-send [enable|disable]
set format {option1}, {option2}, ...
set max-pdf-report {integer}
set options {option1}, {option2}, ...
config page
    Description: Configure report page.
    set paper [a4|letter]
    set column-break-before {option1}, {option2}, ...
    set page-break-before {option1}, {option2}, ...
    set options {option1}, {option2}, ...
    config header
        Description: Configure report page header.
        set style {string}
        config header-item
            Description: Configure report header item.
            edit <id>
                set description {string}
                set type [text|image]
                set style {string}
                set content {string}
                set img-src {string}
            next
        end
    end
    config footer
        Description: Configure report page footer.
        set style {string}
        config footer-item
            Description: Configure report footer item.
            edit <id>
                set description {string}
                set type [text|image]
                set style {string}
                set content {string}
                set img-src {string}
            next
        end
    end
end

```

```

        end
        set schedule-type [demand|daily|...]
        set style-theme {string}
        set subtitle {string}
        set time {user}
        set title {string}
    next
end

```

## config report layout

Parameter	Description	Type	Size	Default
cutoff-option	Cutoff-option is either run-time or custom.	option	-	run-time
	<b>Option</b>	<b>Description</b>		
	<i>run-time</i>	Run time.		
	<i>custom</i>	Custom.		
cutoff-time	Custom cutoff time to generate report (format = hh:mm).	user	Not Specified	
day	Schedule days of week to generate report.	option	-	sunday
	<b>Option</b>	<b>Description</b>		
	<i>sunday</i>	Sunday.		
	<i>monday</i>	Monday.		
	<i>tuesday</i>	Tuesday.		
	<i>wednesday</i>	Wednesday.		
	<i>thursday</i>	Thursday.		
	<i>friday</i>	Friday.		
	<i>saturday</i>	Saturday.		
description	Description.	string	Maximum length: 127	
email-recipients	Email recipients for generated reports.	string	Maximum length: 511	
email-send	Enable/disable sending emails after reports are generated.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable sending emails after generating reports.		
	<i>disable</i>	Disable sending emails after generating reports.		

Parameter	Description	Type	Size	Default												
format	Report format.	option	-	pdf												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>pdf</td><td>PDF.</td></tr></table>				Option	Description	pdf	PDF.								
	Option	Description														
pdf	PDF.															
max-pdf-report	Maximum number of PDF reports to keep at one time (oldest report is overwritten).	integer	Minimum value: 1 Maximum value: 365	31												
name	Report layout name.	string	Maximum length: 35													
options	Report layout options.	option	-	include-table-of-content auto-numbering- heading view- chart-as- heading												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>include-table-of-content</td><td>Include table of content in the report.</td></tr><tr><td>auto-numbering-heading</td><td>Prepend heading with auto numbering.</td></tr><tr><td>view-chart-as-heading</td><td>Auto add heading for each chart.</td></tr><tr><td>show-html-navbar-before-heading</td><td>Show HTML navigation bar before each heading.</td></tr><tr><td>dummy-option</td><td>Use this option if you need none of the above options.</td></tr></table>				Option	Description	include-table-of-content	Include table of content in the report.	auto-numbering-heading	Prepend heading with auto numbering.	view-chart-as-heading	Auto add heading for each chart.	show-html-navbar-before-heading	Show HTML navigation bar before each heading.	dummy-option	Use this option if you need none of the above options.
	Option	Description														
	include-table-of-content	Include table of content in the report.														
	auto-numbering-heading	Prepend heading with auto numbering.														
	view-chart-as-heading	Auto add heading for each chart.														
	show-html-navbar-before-heading	Show HTML navigation bar before each heading.														
dummy-option	Use this option if you need none of the above options.															
schedule-type	Report schedule type.	option	-	daily												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>demand</td><td>Run on demand.</td></tr><tr><td>daily</td><td>Schedule daily.</td></tr><tr><td>weekly</td><td>Schedule weekly.</td></tr></table>				Option	Description	demand	Run on demand.	daily	Schedule daily.	weekly	Schedule weekly.				
	Option	Description														
	demand	Run on demand.														
	daily	Schedule daily.														
weekly	Schedule weekly.															
style-theme	Report style theme.	string	Maximum length: 35													

Parameter	Description	Type	Size	Default
subtitle	Report subtitle.	string	Maximum length: 127	
time	Schedule time to generate report (format = hh:mm).	user	Not Specified	
title	Report title.	string	Maximum length: 127	

### config body-item

Parameter	Description	Type	Size	Default										
id	Report item ID.	integer	Minimum value: 0 Maximum value: 4294967295	0										
description	Description.	string	Maximum length: 63											
type	Report item type.	option	-	text										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>text</i></td><td>Text.</td></tr><tr><td><i>image</i></td><td>Image.</td></tr><tr><td><i>chart</i></td><td>Chart.</td></tr><tr><td><i>misc</i></td><td>Miscellaneous.</td></tr></table>				Option	Description	<i>text</i>	Text.	<i>image</i>	Image.	<i>chart</i>	Chart.	<i>misc</i>	Miscellaneous.
	Option	Description												
	<i>text</i>	Text.												
	<i>image</i>	Image.												
	<i>chart</i>	Chart.												
	<i>misc</i>	Miscellaneous.												
style	Report item style.	string	Maximum length: 71											
top-n	Value of top.	integer	Minimum value: 0 Maximum value: 4294967295	0										
text-component	Report item text component.	option	-	text										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>text</i></td><td>Normal text.</td></tr><tr><td><i>heading1</i></td><td>Heading 1.</td></tr></table>				Option	Description	<i>text</i>	Normal text.	<i>heading1</i>	Heading 1.				
	Option	Description												
	<i>text</i>	Normal text.												
<i>heading1</i>	Heading 1.													

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>heading2</i>	Heading 2.		
	<i>heading3</i>	Heading 3.		
content	Report item text content.	string	Maximum length: 511	
img-src	Report item image file name.	string	Maximum length: 127	
chart	Report item chart name.	string	Maximum length: 71	
chart-options	Report chart options.	option	-	include-no-data hide-title show-caption
	<b>Option</b>	<b>Description</b>		
	<i>include-no-data</i>	Include chart with no data.		
	<i>hide-title</i>	Hide chart title.		
	<i>show-caption</i>	Show chart caption.		
misc-component	Report item miscellaneous component.	option	-	hline
	<b>Option</b>	<b>Description</b>		
	<i>hline</i>	Horizontal line.		
	<i>page-break</i>	Page break.		
	<i>column-break</i>	Column break.		
	<i>section-start</i>	Section start.		
title	Report section title.	string	Maximum length: 511	

### config parameters

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0

Parameter	Description	Type	Size	Default
name	Field name that match field of parameters defined in dataset.	string	Maximum length: 127	
value	Value to replace corresponding field of parameters defined in dataset.	string	Maximum length: 1023	

## config page

Parameter	Description	Type	Size	Default								
paper	Report page paper.	option	-	a4								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>a4</i></td><td>A4 paper.</td></tr><tr><td><i>letter</i></td><td>Letter paper.</td></tr></table>	Option	Description	<i>a4</i>	A4 paper.	<i>letter</i>	Letter paper.					
Option	Description											
<i>a4</i>	A4 paper.											
<i>letter</i>	Letter paper.											
column-break-before	Report page auto column break before heading.	option	-									
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>heading1</i></td><td>Column break before heading 1.</td></tr><tr><td><i>heading2</i></td><td>Column break before heading 2.</td></tr><tr><td><i>heading3</i></td><td>Column break before heading 3.</td></tr></table>	Option	Description	<i>heading1</i>	Column break before heading 1.	<i>heading2</i>	Column break before heading 2.	<i>heading3</i>	Column break before heading 3.			
Option	Description											
<i>heading1</i>	Column break before heading 1.											
<i>heading2</i>	Column break before heading 2.											
<i>heading3</i>	Column break before heading 3.											
page-break-before	Report page auto page break before heading.	option	-									
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>heading1</i></td><td>Page break before heading 1.</td></tr><tr><td><i>heading2</i></td><td>Page break before heading 2.</td></tr><tr><td><i>heading3</i></td><td>Page break before heading 3.</td></tr></table>	Option	Description	<i>heading1</i>	Page break before heading 1.	<i>heading2</i>	Page break before heading 2.	<i>heading3</i>	Page break before heading 3.			
Option	Description											
<i>heading1</i>	Page break before heading 1.											
<i>heading2</i>	Page break before heading 2.											
<i>heading3</i>	Page break before heading 3.											
options	Report page options.	option	-									
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>header-on-first-page</i></td><td>Show header on first page.</td></tr><tr><td><i>footer-on-first-page</i></td><td>Show footer on first page.</td></tr></table>	Option	Description	<i>header-on-first-page</i>	Show header on first page.	<i>footer-on-first-page</i>	Show footer on first page.					
Option	Description											
<i>header-on-first-page</i>	Show header on first page.											
<i>footer-on-first-page</i>	Show footer on first page.											



### config header

Parameter	Description	Type	Size	Default
style	Report header style.	string	Maximum length: 71	

### config header-item

Parameter	Description	Type	Size	Default						
id	Report item ID.	integer	Minimum value: 0 Maximum value: 4294967295	0						
description	Description.	string	Maximum length: 63							
type	Report item type.	option	-	text						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>text</i></td><td>Text.</td></tr><tr><td><i>image</i></td><td>Image.</td></tr></table>				Option	Description	<i>text</i>	Text.	<i>image</i>	Image.
	Option	Description								
	<i>text</i>	Text.								
<i>image</i>	Image.									
style	Report item style.	string	Maximum length: 71							
content	Report item text content.	string	Maximum length: 511							
img-src	Report item image file name.	string	Maximum length: 127							

### config footer

Parameter	Description	Type	Size	Default
style	Report footer style.	string	Maximum length: 71	

## config footer-item

Parameter	Description	Type	Size	Default						
id	Report item ID.	integer	Minimum value: 0 Maximum value: 4294967295	0						
description	Description.	string	Maximum length: 63							
type	Report item type.	option	-	text						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>text</i></td><td>Text.</td></tr><tr><td><i>image</i></td><td>Image.</td></tr></table>				Option	Description	<i>text</i>	Text.	<i>image</i>	Image.
Option	Description									
<i>text</i>	Text.									
<i>image</i>	Image.									
style	Report item style.	string	Maximum length: 71							
content	Report item text content.	string	Maximum length: 511							
img-src	Report item image file name.	string	Maximum length: 127							

## config report setting



This command is available for model(s): FortiGate 1000D, FortiGate 101E, FortiGate 101F, FortiGate 1101E, FortiGate 1200D, FortiGate 1500DT, FortiGate 1500D, FortiGate 1801F, FortiGate 2000E, FortiGate 201E, FortiGate 201F, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3001F, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3301E, FortiGate 3401E, FortiGate 3501F, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 401E, FortiGate 401F, FortiGate 4201F, FortiGate 4401F, FortiGate 5001E1, FortiGate 501E, FortiGate 601E, FortiGate 601F, FortiGate 61E, FortiGate 61F, FortiGate 71F, FortiGate 800D, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 91E, FortiGate VM64, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 1100E, FortiGate 140E-POE, FortiGate 140E, FortiGate 1800F, FortiGate 200E, FortiGate 200F, FortiGate 2200E, FortiGate 3000F, FortiGate 300E, FortiGate 3300E, FortiGate 3400E, FortiGate 3500F, FortiGate 3600E, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4400F, FortiGate 5001E, FortiGate 500E, FortiGate 600E, FortiGate 600F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 70F, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 90E, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 80F 2R.

Report setting configuration.

```
config report setting
  Description: Report setting configuration.
  set fortiview [enable|disable]
  set pdf-report [enable|disable]
  set report-source {option1}, {option2}, ...
  set top-n {integer}
  set web-browsing-threshold {integer}
end
```

## config report setting

Parameter	Description	Type	Size	Default
fortiview	Enable/disable historical FortiView.	option	-	enable **
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable historical FortiView.		
	<i>disable</i>	Disable historical FortiView.		
pdf-report	Enable/disable PDF report.	option	-	enable **

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable PDF report.</td></tr><tr><td><i>disable</i></td><td>Disable PDF report.</td></tr></table>	Option	Description	<i>enable</i>	Enable PDF report.	<i>disable</i>	Disable PDF report.					
	Option	Description										
	<i>enable</i>	Enable PDF report.										
<i>disable</i>	Disable PDF report.											
report-source	Report log source.	option	-	forward-traffic								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>forward-traffic</i></td><td>Report includes forward traffic logs.</td></tr><tr><td><i>sniffer-traffic</i></td><td>Report includes sniffer traffic logs.</td></tr><tr><td><i>local-deny-traffic</i></td><td>Report includes local deny traffic logs.</td></tr></table>	Option	Description	<i>forward-traffic</i>	Report includes forward traffic logs.	<i>sniffer-traffic</i>	Report includes sniffer traffic logs.	<i>local-deny-traffic</i>	Report includes local deny traffic logs.			
	Option	Description										
	<i>forward-traffic</i>	Report includes forward traffic logs.										
	<i>sniffer-traffic</i>	Report includes sniffer traffic logs.										
<i>local-deny-traffic</i>	Report includes local deny traffic logs.											
top-n	Number of items to populate.	integer	Minimum value: 1000 Maximum value: 20000	1000								
web-browsing-threshold	Web browsing time calculation threshold.	integer	Minimum value: 3 Maximum value: 15	3								

\*\* Values may differ between models.

## router

This section includes syntax for the following commands:

- [config router access-list on page 753](#)
- [config router access-list6 on page 754](#)
- [config router aspath-list on page 756](#)
- [config router auth-path on page 757](#)
- [config router bfd on page 757](#)
- [config router bfd6 on page 759](#)
- [config router bgp on page 760](#)
- [config router community-list on page 802](#)
- [config router isis on page 803](#)
- [config router key-chain on page 817](#)
- [config router multicast-flow on page 818](#)
- [config router multicast on page 819](#)
- [config router multicast6 on page 828](#)
- [config router ospf on page 830](#)
- [config router ospf6 on page 846](#)
- [config router policy on page 861](#)
- [config router policy6 on page 864](#)
- [config router prefix-list on page 866](#)
- [config router prefix-list6 on page 867](#)
- [config router rip on page 868](#)
- [config router ripng on page 875](#)
- [config router route-map on page 881](#)
- [config router setting on page 887](#)
- [config router static on page 887](#)
- [config router static6 on page 890](#)

## config router access-list

Configure access lists.

```
config router access-list
  Description: Configure access lists.
  edit <name>
    set comments {string}
    config rule
      Description: Rule.
      edit <id>
        set action [permit|deny]
        set prefix {user}
```

```

        set wildcard {user}
        set exact-match [enable|disable]
    next
end
next
end

```

## config router access-list

Parameter	Description	Type	Size	Default
comments	Comment.	string	Maximum length: 127	
name	Name.	string	Maximum length: 35	

## config rule

Parameter	Description	Type	Size	Default						
id	Rule ID.	integer	Minimum value: 0 Maximum value: 4294967295	0						
action	Permit or deny this IP address and netmask prefix.	option	-	permit						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>permit</i></td><td>Permit or allow this IP address and netmask prefix.</td></tr><tr><td><i>deny</i></td><td>Deny this IP address and netmask prefix.</td></tr></table>				Option	Description	<i>permit</i>	Permit or allow this IP address and netmask prefix.	<i>deny</i>	Deny this IP address and netmask prefix.
	Option	Description								
	<i>permit</i>	Permit or allow this IP address and netmask prefix.								
<i>deny</i>	Deny this IP address and netmask prefix.									
prefix	IPv4 prefix to define regular filter criteria, such as "any" or subnets.	user	Not Specified							
wildcard	Wildcard to define Cisco-style wildcard filter criteria.	user	Not Specified							
exact-match	Enable/disable exact match.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable exact match.</td></tr><tr><td><i>disable</i></td><td>Disable exact match.</td></tr></table>				Option	Description	<i>enable</i>	Enable exact match.	<i>disable</i>	Disable exact match.
	Option	Description								
	<i>enable</i>	Enable exact match.								
<i>disable</i>	Disable exact match.									

## config router access-list6

Configure IPv6 access lists.

```

config router access-list6
  Description: Configure IPv6 access lists.
  edit <name>
    set comments {string}
    config rule
      Description: Rule.
      edit <id>
        set action [permit|deny]
        set prefix6 {user}
        set exact-match [enable|disable]
        set flags {integer}
      next
    end
  next
end

```

### config router access-list6

Parameter	Description	Type	Size	Default
comments	Comment.	string	Maximum length: 127	
name	Name.	string	Maximum length: 35	

### config rule

Parameter	Description	Type	Size	Default						
id	Rule ID.	integer	Minimum value: 0 Maximum value: 4294967295	0						
action	Permit or deny this IP address and netmask prefix.	option	-	permit						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>permit</i></td><td>Permit or allow this IP address and netmask prefix.</td></tr><tr><td><i>deny</i></td><td>Deny this IP address and netmask prefix.</td></tr></table>				Option	Description	<i>permit</i>	Permit or allow this IP address and netmask prefix.	<i>deny</i>	Deny this IP address and netmask prefix.
	Option	Description								
	<i>permit</i>	Permit or allow this IP address and netmask prefix.								
<i>deny</i>	Deny this IP address and netmask prefix.									
prefix6	IPv6 prefix to define regular filter criteria, such as "any" or subnets.	user	Not Specified							
exact-match	Enable/disable exact prefix match.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable exact match.</td></tr><tr><td><i>disable</i></td><td>Disable exact match.</td></tr></table>				Option	Description	<i>enable</i>	Enable exact match.	<i>disable</i>	Disable exact match.
	Option	Description								
	<i>enable</i>	Enable exact match.								
<i>disable</i>	Disable exact match.									

Parameter	Description	Type	Size	Default
flags	Flags.	integer	Minimum value: 0 Maximum value: 4294967295	0

## config router aspath-list

Configure Autonomous System (AS) path lists.

```

config router aspath-list
    Description: Configure Autonomous System (AS) path lists.
    edit <name>
        config rule
            Description: AS path list rule.
            edit <id>
                set action [deny|permit]
                set regexp {string}
            next
        end
    next
end

```

## config router aspath-list

Parameter	Description	Type	Size	Default
name	AS path list name.	string	Maximum length: 35	

## config rule

Parameter	Description	Type	Size	Default						
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0						
action	Permit or deny route-based operations, based on the route's AS_PATH attribute.	option	-							
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>deny</i></td><td>Deny route-based operations.</td></tr><tr><td><i>permit</i></td><td>Permit route-based operations.</td></tr></table>				Option	Description	<i>deny</i>	Deny route-based operations.	<i>permit</i>	Permit route-based operations.
Option	Description									
<i>deny</i>	Deny route-based operations.									
<i>permit</i>	Permit route-based operations.									



Parameter	Description	Type	Size	Default
regex	Regular-expression to match the Border Gateway Protocol (BGP) AS paths.	string	Maximum length: 63	

## config router auth-path

Configure authentication based routing.

```
config router auth-path
    Description: Configure authentication based routing.
    edit <name>
        set device {string}
        set gateway {ipv4-address}
    next
end
```

## config router auth-path

Parameter	Description	Type	Size	Default
device	Outgoing interface.	string	Maximum length: 35	
gateway	Gateway IP address.	ipv4-address	Not Specified	0.0.0.0
name	Name of the entry.	string	Maximum length: 15	

## config router bfd

Configure BFD.

```
config router bfd
    Description: Configure BFD.
    config multihop-template
        Description: BFD multi-hop template table.
        edit <id>
            set src {ipv4-classnet}
            set dst {ipv4-classnet}
            set bfd-desired-min-tx {integer}
            set bfd-required-min-rx {integer}
            set bfd-detect-mult {integer}
            set auth-mode [none|md5]
            set md5-key {password}
        next
    end
    config neighbor
        Description: Neighbor.
        edit <ip>
```

```

        set interface {string}
    next
end
end

```

## config multihop-template

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
src	Source prefix.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0
dst	Destination prefix.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0
bfd-desired-min-tx	BFD desired minimal transmit interval (milliseconds).	integer	Minimum value: 100 Maximum value: 30000	250
bfd-required-min-rx	BFD required minimal receive interval (milliseconds).	integer	Minimum value: 100 Maximum value: 30000	250
bfd-detect-mult	BFD detection multiplier.	integer	Minimum value: 3 Maximum value: 50	3
auth-mode	Authentication mode.	option	-	none
	<b>Option</b> <b>Description</b>			
	<i>none</i>	None.		
	<i>md5</i>	Meticulous MD5 mode.		
md5-key	MD5 key of key ID 1.	password	Not Specified	

## config neighbor

Parameter	Description	Type	Size	Default
ip	IPv4 address of the BFD neighbor.	ipv4-address	Not Specified	0.0.0.0
interface	Interface name.	string	Maximum length: 15	

## config router bfd6

Configure IPv6 BFD.

```
config router bfd6
  Description: Configure IPv6 BFD.
  config multihop-template
    Description: BFD IPv6 multi-hop template table.
    edit <id>
      set src {ipv6-network}
      set dst {ipv6-network}
      set bfd-desired-min-tx {integer}
      set bfd-required-min-rx {integer}
      set bfd-detect-mult {integer}
      set auth-mode [none|md5]
      set md5-key {password}
    next
  end
  config neighbor
    Description: Configure neighbor of IPv6 BFD.
    edit <ip6-address>
      set interface {string}
    next
  end
end
```

## config multihop-template

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
src	Source prefix.	ipv6-network	Not Specified	::/0
dst	Destination prefix.	ipv6-network	Not Specified	::/0
bfd-desired-min-tx	BFD desired minimal transmit interval (milliseconds).	integer	Minimum value: 100 Maximum value: 30000	250
bfd-required-min-rx	BFD required minimal receive interval (milliseconds).	integer	Minimum value: 100 Maximum value: 30000	250

Parameter	Description	Type	Size	Default
bfd-detect-mult	BFD detection multiplier.	integer	Minimum value: 3 Maximum value: 50	3
auth-mode	Authentication mode.	option	-	none
	Option	Description		
	none	None.		
	md5	Meticulous MD5 mode.		
md5-key	MD5 key of key ID 1.	password	Not Specified	

## config neighbor

Parameter	Description	Type	Size	Default
ip6-address	IPv6 address of the BFD neighbor.	ipv6-address	Not Specified	::
interface	Interface to the BFD neighbor.	string	Maximum length: 15	

## config router bgp

Configure BGP.

```

config router bgp
  Description: Configure BGP.
  set additional-path [enable|disable]
  set additional-path-select {integer}
  set additional-path-select6 {integer}
  set additional-path6 [enable|disable]
  config admin-distance
    Description: Administrative distance modifications.
    edit <id>
      set neighbour-prefix {ipv4-classnet}
      set route-list {string}
      set distance {integer}
    next
  end
  config aggregate-address
    Description: BGP aggregate address table.
    edit <id>
      set prefix {ipv4-classnet-any}
      set as-set [enable|disable]
      set summary-only [enable|disable]
    next
  end
  config aggregate-address6

```

```

Description: BGP IPv6 aggregate address table.
edit <id>
    set prefix6 {ipv6-prefix}
    set as-set [enable|disable]
    set summary-only [enable|disable]
next
end
set always-compare-med [enable|disable]
set as {integer}
set bestpath-as-path-ignore [enable|disable]
set bestpath-cmp-confed-aspath [enable|disable]
set bestpath-cmp-routerid [enable|disable]
set bestpath-med-confed [enable|disable]
set bestpath-med-missing-as-worst [enable|disable]
set client-to-client-reflection [enable|disable]
set cluster-id {ipv4-address-any}
set confederation-identifier {integer}
set confederation-peers <peer1>, <peer2>, ...
set dampening [enable|disable]
set dampening-max-suppress-time {integer}
set dampening-reachability-half-life {integer}
set dampening-reuse {integer}
set dampening-route-map {string}
set dampening-suppress {integer}
set dampening-unreachability-half-life {integer}
set default-local-preference {integer}
set deterministic-med [enable|disable]
set distance-external {integer}
set distance-internal {integer}
set distance-local {integer}
set ebgp-multipath [enable|disable]
set enforce-first-as [enable|disable]
set fast-external-failover [enable|disable]
set graceful-end-on-timer [enable|disable]
set graceful-restart [enable|disable]
set graceful-restart-time {integer}
set graceful-stalepath-time {integer}
set graceful-update-delay {integer}
set holdtime-timer {integer}
set ibgp-multipath [enable|disable]
set ignore-optional-capability [enable|disable]
set keepalive-timer {integer}
set log-neighbour-changes [enable|disable]
set multipath-recursive-distance [enable|disable]
config neighbor
Description: BGP neighbor table.
edit <ip>
    set advertisement-interval {integer}
    set allowas-in-enable [enable|disable]
    set allowas-in-enable6 [enable|disable]
    set allowas-in {integer}
    set allowas-in6 {integer}
    set attribute-unchanged {option1}, {option2}, ...
    set attribute-unchanged6 {option1}, {option2}, ...
    set activate [enable|disable]
    set activate6 [enable|disable]

```

---

```
set bfd [enable|disable]
set capability-dynamic [enable|disable]
set capability-orf [none|receive|...]
set capability-orf6 [none|receive|...]
set capability-graceful-restart [enable|disable]
set capability-graceful-restart6 [enable|disable]
set capability-route-refresh [enable|disable]
set capability-default-originate [enable|disable]
set capability-default-originate6 [enable|disable]
set dont-capability-negotiate [enable|disable]
set ebgp-enforce-multihop [enable|disable]
set link-down-failover [enable|disable]
set stale-route [enable|disable]
set next-hop-self [enable|disable]
set next-hop-self6 [enable|disable]
set next-hop-self-rr [enable|disable]
set next-hop-self-rr6 [enable|disable]
set override-capability [enable|disable]
set passive [enable|disable]
set remove-private-as [enable|disable]
set remove-private-as6 [enable|disable]
set route-reflector-client [enable|disable]
set route-reflector-client6 [enable|disable]
set route-server-client [enable|disable]
set route-server-client6 [enable|disable]
set shutdown [enable|disable]
set soft-reconfiguration [enable|disable]
set soft-reconfiguration6 [enable|disable]
set as-override [enable|disable]
set as-override6 [enable|disable]
set strict-capability-match [enable|disable]
set default-originate-routemap {string}
set default-originate-routemap6 {string}
set description {string}
set distribute-list-in {string}
set distribute-list-in6 {string}
set distribute-list-out {string}
set distribute-list-out6 {string}
set ebgp-multihop-ttl {integer}
set filter-list-in {string}
set filter-list-in6 {string}
set filter-list-out {string}
set filter-list-out6 {string}
set interface {string}
set maximum-prefix {integer}
set maximum-prefix6 {integer}
set maximum-prefix-threshold {integer}
set maximum-prefix-threshold6 {integer}
set maximum-prefix-warning-only [enable|disable]
set maximum-prefix-warning-only6 [enable|disable]
set prefix-list-in {string}
set prefix-list-in6 {string}
set prefix-list-out {string}
set prefix-list-out6 {string}
set remote-as {integer}
set local-as {integer}
```

```

set local-as-no-prepend [enable|disable]
set local-as-replace-as [enable|disable]
set retain-stale-time {integer}
set route-map-in {string}
set route-map-in6 {string}
set route-map-out {string}
set route-map-out-preferable {string}
set route-map-out6 {string}
set route-map-out6-preferable {string}
set send-community [standard|extended|...]
set send-community6 [standard|extended|...]
set keep-alive-timer {integer}
set holdtime-timer {integer}
set connect-timer {integer}
set unsuppress-map {string}
set unsuppress-map6 {string}
set update-source {string}
set weight {integer}
set restart-time {integer}
set additional-path [send|receive|...]
set additional-path6 [send|receive|...]
set adv-additional-path {integer}
set adv-additional-path6 {integer}
set password {password}
config conditional-advertise
    Description: Conditional advertisement.
    edit <advertise-routemap>
        set condition-routemap <name1>, <name2>, ...
        set condition-type [exist|non-exist]
    next
end
config conditional-advertise6
    Description: IPv6 conditional advertisement.
    edit <advertise-routemap>
        set condition-routemap <name1>, <name2>, ...
        set condition-type [exist|non-exist]
    next
end
next
end
config neighbor-group
    Description: BGP neighbor group table.
    edit <name>
        set advertisement-interval {integer}
        set allowas-in-enable [enable|disable]
        set allowas-in-enable6 [enable|disable]
        set allowas-in {integer}
        set allowas-in6 {integer}
        set attribute-unchanged {option1}, {option2}, ...
        set attribute-unchanged6 {option1}, {option2}, ...
        set activate [enable|disable]
        set activate6 [enable|disable]
        set bfd [enable|disable]
        set capability-dynamic [enable|disable]
        set capability-orf [none|receive|...]
        set capability-orf6 [none|receive|...]
    end
end

```

---

```
set capability-graceful-restart [enable|disable]
set capability-graceful-restart6 [enable|disable]
set capability-route-refresh [enable|disable]
set capability-default-originate [enable|disable]
set capability-default-originate6 [enable|disable]
set dont-capability-negotiate [enable|disable]
set ebgp-enforce-multihop [enable|disable]
set link-down-failover [enable|disable]
set stale-route [enable|disable]
set next-hop-self [enable|disable]
set next-hop-self6 [enable|disable]
set next-hop-self-rr [enable|disable]
set next-hop-self-rr6 [enable|disable]
set override-capability [enable|disable]
set passive [enable|disable]
set remove-private-as [enable|disable]
set remove-private-as6 [enable|disable]
set route-reflector-client [enable|disable]
set route-reflector-client6 [enable|disable]
set route-server-client [enable|disable]
set route-server-client6 [enable|disable]
set shutdown [enable|disable]
set soft-reconfiguration [enable|disable]
set soft-reconfiguration6 [enable|disable]
set as-override [enable|disable]
set as-override6 [enable|disable]
set strict-capability-match [enable|disable]
set default-originate-routemap {string}
set default-originate-routemap6 {string}
set description {string}
set distribute-list-in {string}
set distribute-list-in6 {string}
set distribute-list-out {string}
set distribute-list-out6 {string}
set ebgp-multihop-ttl {integer}
set filter-list-in {string}
set filter-list-in6 {string}
set filter-list-out {string}
set filter-list-out6 {string}
set interface {string}
set maximum-prefix {integer}
set maximum-prefix6 {integer}
set maximum-prefix-threshold {integer}
set maximum-prefix-threshold6 {integer}
set maximum-prefix-warning-only [enable|disable]
set maximum-prefix-warning-only6 [enable|disable]
set prefix-list-in {string}
set prefix-list-in6 {string}
set prefix-list-out {string}
set prefix-list-out6 {string}
set remote-as {integer}
set local-as {integer}
set local-as-no-prepend [enable|disable]
set local-as-replace-as [enable|disable]
set retain-stale-time {integer}
set route-map-in {string}
```



```

        set route-map-in6 {string}
        set route-map-out {string}
        set route-map-out-preferable {string}
        set route-map-out6 {string}
        set route-map-out6-preferable {string}
        set send-community [standard|extended|...]
        set send-community6 [standard|extended|...]
        set keep-alive-timer {integer}
        set holdtime-timer {integer}
        set connect-timer {integer}
        set unsuppress-map {string}
        set unsuppress-map6 {string}
        set update-source {string}
        set weight {integer}
        set restart-time {integer}
        set additional-path [send|receive|...]
        set additional-path6 [send|receive|...]
        set adv-additional-path {integer}
        set adv-additional-path6 {integer}
    next
end
config neighbor-range
    Description: BGP neighbor range table.
    edit <id>
        set prefix {ipv4-classnet}
        set max-neighbor-num {integer}
        set neighbor-group {string}
    next
end
config neighbor-range6
    Description: BGP IPv6 neighbor range table.
    edit <id>
        set prefix6 {ipv6-network}
        set max-neighbor-num {integer}
        set neighbor-group {string}
    next
end
config network
    Description: BGP network table.
    edit <id>
        set prefix {ipv4-classnet}
        set network-import-check [global|enable|...]
        set backdoor [enable|disable]
        set route-map {string}
    next
end
set network-import-check [enable|disable]
config network6
    Description: BGP IPv6 network table.
    edit <id>
        set prefix6 {ipv6-network}
        set network-import-check [global|enable|...]
        set backdoor [enable|disable]
        set route-map {string}
    next
end

```

```

set recursive-next-hop [enable|disable]
config redistribute
    Description: BGP IPv4 redistribute table.
    edit <name>
        set status [enable|disable]
        set route-map {string}
    next
end
config redistribute6
    Description: BGP IPv6 redistribute table.
    edit <name>
        set status [enable|disable]
        set route-map {string}
    next
end
set router-id {ipv4-address-any}
set scan-time {integer}
set synchronization [enable|disable]
set tag-resolve-mode [disable|preferred|...]
config vrf-leak
    Description: BGP VRF leaking table.
    edit <vrf>
        config target
            Description: Target VRF table.
            edit <vrf>
                set route-map {string}
                set interface {string}
            next
        end
    next
end
config vrf-leak6
    Description: BGP IPv6 VRF leaking table.
    edit <vrf>
        config target
            Description: Target VRF table.
            edit <vrf>
                set route-map {string}
                set interface {string}
            next
        end
    next
end
end

```

## config router bgp

Parameter	Description	Type	Size	Default
additional-path	Enable/disable selection of BGP IPv4 additional paths.	option	-	disable

Parameter	Description	Type	Size	Default
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
additional-path-select	Number of additional paths to be selected for each IPv4 NLRI.	integer	Minimum value: 2 Maximum value: 255	2
additional-path-select6	Number of additional paths to be selected for each IPv6 NLRI.	integer	Minimum value: 2 Maximum value: 255	2
additional-path6	Enable/disable selection of BGP IPv6 additional paths.	option	-	disable
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
always-compare-med	Enable/disable always compare MED.	option	-	disable
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
as	Router AS number, valid from 1 to 4294967295, 0 to disable BGP.	integer	Minimum value: 0 Maximum value: 4294967295	0
bestpath-as-path-ignore	Enable/disable ignore AS path.	option	-	disable
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
bestpath-cmp-confed-aspath	Enable/disable compare federation AS path length.	option	-	disable

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
bestpath-cmp-routerid	Enable/disable compare router ID for identical EBGP paths.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
bestpath-med-confed	Enable/disable compare MED among confederation paths.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
bestpath-med-missing-as-worst	Enable/disable treat missing MED as least preferred.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
client-to-client-reflection	Enable/disable client-to-client route reflection.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
cluster-id	Route reflector cluster ID.	ipv4-address-any	Not Specified	0.0.0.0
confederation-identifier	Confederation identifier.	integer	Minimum value: 1 Maximum value: 4294967295	0

Parameter	Description	Type	Size	Default
confederation-peers <peer>	Confederation peers. Peer ID.	string	Maximum length: 79	
dampening	Enable/disable route-flap dampening.	option	-	disable
	Option	Description		
	enable	Enable setting.		
	disable	Disable setting.		
dampening-max-suppress-time	Maximum minutes a route can be suppressed.	integer	Minimum value: 1 Maximum value: 255	60
dampening-reachability-half-life	Reachability half-life time for penalty (min).	integer	Minimum value: 1 Maximum value: 45	15
dampening-reuse	Threshold to reuse routes.	integer	Minimum value: 1 Maximum value: 20000	750
dampening-route-map	Criteria for dampening.	string	Maximum length: 35	
dampening-suppress	Threshold to suppress routes.	integer	Minimum value: 1 Maximum value: 20000	2000
dampening-unreachability-half-life	Unreachability half-life time for penalty (min).	integer	Minimum value: 1 Maximum value: 45	15
default-local-preference	Default local preference.	integer	Minimum value: 0 Maximum value: 4294967295	100
deterministic-med	Enable/disable enforce deterministic comparison of MED.	option	-	disable
	Option	Description		
	enable	Enable setting.		

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable setting.		
distance-external	Distance for routes external to the AS.	integer	Minimum value: 1 Maximum value: 255	20
distance-internal	Distance for routes internal to the AS.	integer	Minimum value: 1 Maximum value: 255	200
distance-local	Distance for routes local to the AS.	integer	Minimum value: 1 Maximum value: 255	200
ebgp-multipath	Enable/disable EBGp multi-path.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
enforce-first-as	Enable/disable enforce first AS for EBGp routes.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
fast-external-failover	Enable/disable reset peer BGP session if link goes down.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
graceful-end-on-timer	Enable/disable to exit graceful restart on timer only.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

Parameter	Description	Type	Size	Default						
graceful-restart	Enable/disable BGP graceful restart capabilities.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>				Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.
	Option	Description								
	<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.									
graceful-restart-time	Time needed for neighbors to restart (sec).	integer	Minimum value: 1 Maximum value: 3600	120						
graceful-stalepath-time	Time to hold stale paths of restarting neighbor (sec).	integer	Minimum value: 1 Maximum value: 3600	360						
graceful-update-delay	Route advertisement/selection delay after restart (sec).	integer	Minimum value: 1 Maximum value: 3600	120						
holdtime-timer	Number of seconds to mark peer as dead.	integer	Minimum value: 3 Maximum value: 65535	180						
ibgp-multipath	Enable/disable IBGP multi-path.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>				Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.
	Option	Description								
	<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.									
ignore-optional-capability	Do not send unknown optional capability notification message.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>				Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.
	Option	Description								
	<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.									
keepalive-timer	Frequency to send keep alive requests.	integer	Minimum value: 0 Maximum value: 65535	60						
log-neighbour-changes	Log BGP neighbor changes.	option	-	enable						

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
multipath-recursive-distance	Enable/disable use of recursive distance to select multipath.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
network-import-check	Enable/disable ensure BGP network route exists in IGP.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
recursive-next-hop	Enable/disable recursive resolution of next-hop using BGP route.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
router-id	Router ID.	ipv4-address-any	Not Specified	
scan-time	Background scanner interval (sec), 0 to disable it.	integer	Minimum value: 5 Maximum value: 60	60
synchronization	Enable/disable only advertise routes from iBGP if routes present in an IGP.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		



Parameter	Description	Type	Size	Default
tag-resolve-mode	Configure tag-match mode. Resolves BGP routes with other routes containing the same tag.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable tag-match mode.		
	<i>preferred</i>	Use tag-match if a BGP route resolution with another route containing the same tag is successful.		
	<i>merge</i>	Merge tag-match with best-match if they are using different routes. The result will exclude the next hops of tag-match whose interfaces have appeared in best-match.		

### config admin-distance

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
neighbour-prefix	Neighbor address prefix.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0
route-list	Access list of routes to apply new distance to.	string	Maximum length: 35	
distance	Administrative distance to apply.	integer	Minimum value: 1 Maximum value: 255	0

### config aggregate-address

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
prefix	Aggregate prefix.	ipv4-classnet-any	Not Specified	0.0.0.0 0.0.0.0
as-set	Enable/disable generate AS set path information.	option	-	disable

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
summary-only	Enable/disable filter more specific routes from updates.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

### config aggregate-address6

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
prefix6	Aggregate IPv6 prefix.	ipv6-prefix	Not Specified	::/0
as-set	Enable/disable generate AS set path information.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
summary-only	Enable/disable filter more specific routes from updates.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

### config neighbor

Parameter	Description	Type	Size	Default
ip	IP/IPv6 address of neighbor.	string	Maximum length: 45	

Parameter	Description	Type	Size	Default								
advertisement-interval	Minimum interval (sec) between sending updates.	integer	Minimum value: 0 Maximum value: 600	30								
allowas-in-enable	Enable/disable IPv4 Enable to allow my AS in AS path.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
allowas-in-enable6	Enable/disable IPv6 Enable to allow my AS in AS path.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
allowas-in	IPv4 The maximum number of occurrence of my AS number allowed.	integer	Minimum value: 1 Maximum value: 10	3								
allowas-in6	IPv6 The maximum number of occurrence of my AS number allowed.	integer	Minimum value: 1 Maximum value: 10	3								
attribute-unchanged	IPv4 List of attributes that should be unchanged.	option	-									
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>as-path</i></td><td>AS path.</td></tr><tr><td><i>med</i></td><td>MED.</td></tr><tr><td><i>next-hop</i></td><td>Next hop.</td></tr></table>	Option	Description	<i>as-path</i>	AS path.	<i>med</i>	MED.	<i>next-hop</i>	Next hop.			
Option	Description											
<i>as-path</i>	AS path.											
<i>med</i>	MED.											
<i>next-hop</i>	Next hop.											
attribute-unchanged6	IPv6 List of attributes that should be unchanged.	option	-									
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>as-path</i></td><td>AS path.</td></tr><tr><td><i>med</i></td><td>MED.</td></tr></table>	Option	Description	<i>as-path</i>	AS path.	<i>med</i>	MED.					
Option	Description											
<i>as-path</i>	AS path.											
<i>med</i>	MED.											

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>next-hop</i>	Next hop.		
activate	Enable/disable address family IPv4 for this neighbor.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
activate6	Enable/disable address family IPv6 for this neighbor.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
bfd	Enable/disable BFD for this neighbor.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
capability-dynamic	Enable/disable advertise dynamic capability to this neighbor.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
capability-orf	Accept/Send IPv4 ORF lists to/from this neighbor.	option	-	none
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	None.		
	<i>receive</i>	Receive ORF lists.		
	<i>send</i>	Send ORF list.		
	<i>both</i>	Send and receive ORF lists.		

Parameter	Description	Type	Size	Default										
capability-orf6	Accept/Send IPv6 ORF lists to/from this neighbor.	option	-	none										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>None.</td></tr><tr><td><i>receive</i></td><td>Receive ORF lists.</td></tr><tr><td><i>send</i></td><td>Send ORF list.</td></tr><tr><td><i>both</i></td><td>Send and receive ORF lists.</td></tr></table>	Option	Description	<i>none</i>	None.	<i>receive</i>	Receive ORF lists.	<i>send</i>	Send ORF list.	<i>both</i>	Send and receive ORF lists.			
Option	Description													
<i>none</i>	None.													
<i>receive</i>	Receive ORF lists.													
<i>send</i>	Send ORF list.													
<i>both</i>	Send and receive ORF lists.													
capability-graceful-restart	Enable/disable advertise IPv4 graceful restart capability to this neighbor.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.							
Option	Description													
<i>enable</i>	Enable setting.													
<i>disable</i>	Disable setting.													
capability-graceful-restart6	Enable/disable advertise IPv6 graceful restart capability to this neighbor.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.							
Option	Description													
<i>enable</i>	Enable setting.													
<i>disable</i>	Disable setting.													
capability-route-refresh	Enable/disable advertise route refresh capability to this neighbor.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.							
Option	Description													
<i>enable</i>	Enable setting.													
<i>disable</i>	Disable setting.													
capability-default-originate	Enable/disable advertise default IPv4 route to this neighbor.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.							
Option	Description													
<i>enable</i>	Enable setting.													
<i>disable</i>	Disable setting.													
capability-default-originate6	Enable/disable advertise default IPv6 route to this neighbor.	option	-	disable										

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
dont-capability-negotiate	Do not negotiate capabilities with this neighbor.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
ebgp-enforce-multihop	Enable/disable allow multi-hop EBGp neighbors.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
link-down-failover	Enable/disable failover upon link down.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
stale-route	Enable/disable stale route after neighbor down.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
next-hop-self	Enable/disable IPv4 next-hop calculation for this neighbor.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
next-hop-self6	Enable/disable IPv6 next-hop calculation for this neighbor.	option	-	disable

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
next-hop-self-rr	Enable/disable setting nexthop's address to interface's IPv4 address for route-reflector routes.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
next-hop-self-rr6	Enable/disable setting nexthop's address to interface's IPv6 address for route-reflector routes.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
override-capability	Enable/disable override result of capability negotiation.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
passive	Enable/disable sending of open messages to this neighbor.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
remove-private-as	Enable/disable remove private AS number from IPv4 outbound updates.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

Parameter	Description	Type	Size	Default						
remove-private-as6	Enable/disable remove private AS number from IPv6 outbound updates.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
route-reflector-client	Enable/disable IPv4 AS route reflector client.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
route-reflector-client6	Enable/disable IPv6 AS route reflector client.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
route-server-client	Enable/disable IPv4 AS route server client.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
route-server-client6	Enable/disable IPv6 AS route server client.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
shutdown	Enable/disable shutdown this neighbor.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									



Parameter	Description	Type	Size	Default						
soft-reconfiguration	Enable/disable allow IPv4 inbound soft reconfiguration.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
soft-reconfiguration6	Enable/disable allow IPv6 inbound soft reconfiguration.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
as-override	Enable/disable replace peer AS with own AS for IPv4.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
as-override6	Enable/disable replace peer AS with own AS for IPv6.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
strict-capability-match	Enable/disable strict capability matching.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
default-originate-routemap	Route map to specify criteria to originate IPv4 default.	string	Maximum length: 35							
default-originate-routemap6	Route map to specify criteria to originate IPv6 default.	string	Maximum length: 35							
description	Description.	string	Maximum length: 63							

Parameter	Description	Type	Size	Default
distribute-list-in	Filter for IPv4 updates from this neighbor.	string	Maximum length: 35	
distribute-list-in6	Filter for IPv6 updates from this neighbor.	string	Maximum length: 35	
distribute-list-out	Filter for IPv4 updates to this neighbor.	string	Maximum length: 35	
distribute-list-out6	Filter for IPv6 updates to this neighbor.	string	Maximum length: 35	
ebgp-multihop-ttl	EBGP multihop TTL for this peer.	integer	Minimum value: 1 Maximum value: 255	255
filter-list-in	BGP filter for IPv4 inbound routes.	string	Maximum length: 35	
filter-list-in6	BGP filter for IPv6 inbound routes.	string	Maximum length: 35	
filter-list-out	BGP filter for IPv4 outbound routes.	string	Maximum length: 35	
filter-list-out6	BGP filter for IPv6 outbound routes.	string	Maximum length: 35	
interface	Specify outgoing interface for peer connection. For IPv6 peer, the interface should have link-local address.	string	Maximum length: 15	
maximum-prefix	Maximum number of IPv4 prefixes to accept from this peer.	integer	Minimum value: 1 Maximum value: 4294967295	0
maximum-prefix6	Maximum number of IPv6 prefixes to accept from this peer.	integer	Minimum value: 1 Maximum value: 4294967295	0
maximum-prefix-threshold	Maximum IPv4 prefix threshold value.	integer	Minimum value: 1 Maximum value: 100	75

Parameter	Description	Type	Size	Default
maximum-prefix-threshold6	Maximum IPv6 prefix threshold value.	integer	Minimum value: 1 Maximum value: 100	75
maximum-prefix-warning-only	Enable/disable IPv4 Only give warning message when limit is exceeded.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
maximum-prefix-warning-only6	Enable/disable IPv6 Only give warning message when limit is exceeded.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
prefix-list-in	IPv4 Inbound filter for updates from this neighbor.	string	Maximum length: 35	
prefix-list-in6	IPv6 Inbound filter for updates from this neighbor.	string	Maximum length: 35	
prefix-list-out	IPv4 Outbound filter for updates to this neighbor.	string	Maximum length: 35	
prefix-list-out6	IPv6 Outbound filter for updates to this neighbor.	string	Maximum length: 35	
remote-as	AS number of neighbor.	integer	Minimum value: 1 Maximum value: 4294967295	0
local-as	Local AS number of neighbor.	integer	Minimum value: 0 Maximum value: 4294967295	0
local-as-no-prepend	Do not prepend local-as to incoming updates.	option	-	disable

Parameter	Description	Type	Size	Default										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.							
	Option	Description												
	<i>enable</i>	Enable setting.												
<i>disable</i>	Disable setting.													
local-as-replace-as	Replace real AS with local-as in outgoing updates.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.							
	Option	Description												
	<i>enable</i>	Enable setting.												
<i>disable</i>	Disable setting.													
retain-stale-time	Time to retain stale routes.	integer	Minimum value: 0 Maximum value: 65535	0										
route-map-in	IPv4 Inbound route map filter.	string	Maximum length: 35											
route-map-in6	IPv6 Inbound route map filter.	string	Maximum length: 35											
route-map-out	IPv4 outbound route map filter.	string	Maximum length: 35											
route-map-out-preferable	IPv4 outbound route map filter if the peer is preferred.	string	Maximum length: 35											
route-map-out6	IPv6 Outbound route map filter.	string	Maximum length: 35											
route-map-out6-preferable	IPv6 outbound route map filter if the peer is preferred.	string	Maximum length: 35											
send-community	IPv4 Send community attribute to neighbor.	option	-	both										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>standard</i></td><td>Standard.</td></tr><tr><td><i>extended</i></td><td>Extended.</td></tr><tr><td><i>both</i></td><td>Both.</td></tr><tr><td><i>disable</i></td><td>Disable</td></tr></table>	Option	Description	<i>standard</i>	Standard.	<i>extended</i>	Extended.	<i>both</i>	Both.	<i>disable</i>	Disable			
	Option	Description												
	<i>standard</i>	Standard.												
	<i>extended</i>	Extended.												
	<i>both</i>	Both.												
<i>disable</i>	Disable													
send-community6	IPv6 Send community attribute to neighbor.	option	-	both										

Parameter	Description	Type	Size	Default
	Option	Description		
	standard	Standard.		
	extended	Extended.		
	both	Both.		
	disable	Disable		
keep-alive-timer	Keep alive timer interval (sec).	integer	Minimum value: 0 Maximum value: 65535	4294967295
holdtime-timer	Interval (sec) before peer considered dead.	integer	Minimum value: 3 Maximum value: 65535	4294967295
connect-timer	Interval (sec) for connect timer.	integer	Minimum value: 0 Maximum value: 65535	4294967295
unsuppress-map	IPv4 Route map to selectively unsuppress suppressed routes.	string	Maximum length: 35	
unsuppress-map6	IPv6 Route map to selectively unsuppress suppressed routes.	string	Maximum length: 35	
update-source	Interface to use as source IP/IPv6 address of TCP connections.	string	Maximum length: 15	
weight	Neighbor weight.	integer	Minimum value: 0 Maximum value: 65535	4294967295
restart-time	Graceful restart delay time.	integer	Minimum value: 0 Maximum value: 3600	0
additional-path	Enable/disable IPv4 additional-path capability.	option	-	disable
	Option	Description		
	send	Enable sending additional paths.		
	receive	Enable receiving additional paths.		

Parameter	Description	Type	Size	Default										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>both</i></td><td>Enable sending and receiving additional paths.</td></tr><tr><td><i>disable</i></td><td>Disable additional paths.</td></tr></table>	Option	Description	<i>both</i>	Enable sending and receiving additional paths.	<i>disable</i>	Disable additional paths.							
	Option	Description												
	<i>both</i>	Enable sending and receiving additional paths.												
<i>disable</i>	Disable additional paths.													
additional-path6	Enable/disable IPv6 additional-path capability.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>send</i></td><td>Enable sending additional paths.</td></tr><tr><td><i>receive</i></td><td>Enable receiving additional paths.</td></tr><tr><td><i>both</i></td><td>Enable sending and receiving additional paths.</td></tr><tr><td><i>disable</i></td><td>Disable additional paths.</td></tr></table>	Option	Description	<i>send</i>	Enable sending additional paths.	<i>receive</i>	Enable receiving additional paths.	<i>both</i>	Enable sending and receiving additional paths.	<i>disable</i>	Disable additional paths.			
	Option	Description												
	<i>send</i>	Enable sending additional paths.												
	<i>receive</i>	Enable receiving additional paths.												
	<i>both</i>	Enable sending and receiving additional paths.												
<i>disable</i>	Disable additional paths.													
adv-additional-path	Number of IPv4 additional paths that can be advertised to this neighbor.	integer	Minimum value: 2 Maximum value: 255	2										
adv-additional-path6	Number of IPv6 additional paths that can be advertised to this neighbor.	integer	Minimum value: 2 Maximum value: 255	2										
password	Password used in MD5 authentication.	password	Not Specified											

### config conditional-advertise

Parameter	Description	Type	Size	Default						
advertise-routemap	Name of advertising route map.	string	Maximum length: 35							
condition-routemap <name>	List of conditional route maps. route map	string	Maximum length: 79							
condition-type	Type of condition.	option	-	exist						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>exist</i></td><td>True if condition route map is matched.</td></tr><tr><td><i>non-exist</i></td><td>True if condition route map is not matched.</td></tr></table>				Option	Description	<i>exist</i>	True if condition route map is matched.	<i>non-exist</i>	True if condition route map is not matched.
Option	Description									
<i>exist</i>	True if condition route map is matched.									
<i>non-exist</i>	True if condition route map is not matched.									

## config conditional-advertise6

Parameter	Description	Type	Size	Default						
advertise-routemap	Name of advertising route map.	string	Maximum length: 35							
condition-routemap <name>	List of conditional route maps. route map	string	Maximum length: 79							
condition-type	Type of condition.	option	-	exist						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>exist</i></td><td>True if condition route map is matched.</td></tr><tr><td><i>non-exist</i></td><td>True if condition route map is not matched.</td></tr></table>				Option	Description	<i>exist</i>	True if condition route map is matched.	<i>non-exist</i>	True if condition route map is not matched.
Option	Description									
<i>exist</i>	True if condition route map is matched.									
<i>non-exist</i>	True if condition route map is not matched.									

## config neighbor-group

Parameter	Description	Type	Size	Default						
name	Neighbor group name.	string	Maximum length: 45							
advertisement-interval	Minimum interval (sec) between sending updates.	integer	Minimum value: 0 Maximum value: 600	30						
allowas-in-enable	Enable/disable IPv4 Enable to allow my AS in AS path.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>				Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
allowas-in-enable6	Enable/disable IPv6 Enable to allow my AS in AS path.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>				Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
allowas-in	IPv4 The maximum number of occurrence of my AS number allowed.	integer	Minimum value: 1 Maximum value: 10	3						

Parameter	Description	Type	Size	Default								
allowas-in6	IPv6 The maximum number of occurrence of my AS number allowed.	integer	Minimum value: 1 Maximum value: 10	3								
attribute-unchanged	IPv4 List of attributes that should be unchanged.	option	-									
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>as-path</i></td><td>AS path.</td></tr><tr><td><i>med</i></td><td>MED.</td></tr><tr><td><i>next-hop</i></td><td>Next hop.</td></tr></table>	Option	Description	<i>as-path</i>	AS path.	<i>med</i>	MED.	<i>next-hop</i>	Next hop.			
Option	Description											
<i>as-path</i>	AS path.											
<i>med</i>	MED.											
<i>next-hop</i>	Next hop.											
attribute-unchanged6	IPv6 List of attributes that should be unchanged.	option	-									
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>as-path</i></td><td>AS path.</td></tr><tr><td><i>med</i></td><td>MED.</td></tr><tr><td><i>next-hop</i></td><td>Next hop.</td></tr></table>	Option	Description	<i>as-path</i>	AS path.	<i>med</i>	MED.	<i>next-hop</i>	Next hop.			
Option	Description											
<i>as-path</i>	AS path.											
<i>med</i>	MED.											
<i>next-hop</i>	Next hop.											
activate	Enable/disable address family IPv4 for this neighbor.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
activate6	Enable/disable address family IPv6 for this neighbor.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
bfd	Enable/disable BFD for this neighbor.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											



Parameter	Description	Type	Size	Default										
capability-dynamic	Enable/disable advertise dynamic capability to this neighbor.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.							
Option	Description													
<i>enable</i>	Enable setting.													
<i>disable</i>	Disable setting.													
capability-orf	Accept/Send IPv4 ORF lists to/from this neighbor.	option	-	none										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>None.</td></tr><tr><td><i>receive</i></td><td>Receive ORF lists.</td></tr><tr><td><i>send</i></td><td>Send ORF list.</td></tr><tr><td><i>both</i></td><td>Send and receive ORF lists.</td></tr></table>	Option	Description	<i>none</i>	None.	<i>receive</i>	Receive ORF lists.	<i>send</i>	Send ORF list.	<i>both</i>	Send and receive ORF lists.			
Option	Description													
<i>none</i>	None.													
<i>receive</i>	Receive ORF lists.													
<i>send</i>	Send ORF list.													
<i>both</i>	Send and receive ORF lists.													
capability-orf6	Accept/Send IPv6 ORF lists to/from this neighbor.	option	-	none										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>None.</td></tr><tr><td><i>receive</i></td><td>Receive ORF lists.</td></tr><tr><td><i>send</i></td><td>Send ORF list.</td></tr><tr><td><i>both</i></td><td>Send and receive ORF lists.</td></tr></table>	Option	Description	<i>none</i>	None.	<i>receive</i>	Receive ORF lists.	<i>send</i>	Send ORF list.	<i>both</i>	Send and receive ORF lists.			
Option	Description													
<i>none</i>	None.													
<i>receive</i>	Receive ORF lists.													
<i>send</i>	Send ORF list.													
<i>both</i>	Send and receive ORF lists.													
capability-graceful-restart	Enable/disable advertise IPv4 graceful restart capability to this neighbor.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.							
Option	Description													
<i>enable</i>	Enable setting.													
<i>disable</i>	Disable setting.													
capability-graceful-restart6	Enable/disable advertise IPv6 graceful restart capability to this neighbor.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.							
Option	Description													
<i>enable</i>	Enable setting.													
<i>disable</i>	Disable setting.													
capability-route-refresh	Enable/disable advertise route refresh capability to this neighbor.	option	-	enable										

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
capability-default-originate	Enable/disable advertise default IPv4 route to this neighbor.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
capability-default-originate6	Enable/disable advertise default IPv6 route to this neighbor.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
dont-capability-negotiate	Do not negotiate capabilities with this neighbor.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
ebgp-enforce-multihop	Enable/disable allow multi-hop EBGp neighbors.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
link-down-failover	Enable/disable failover upon link down.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
stale-route	Enable/disable stale route after neighbor down.	option	-	disable

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
next-hop-self	Enable/disable IPv4 next-hop calculation for this neighbor.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
next-hop-self6	Enable/disable IPv6 next-hop calculation for this neighbor.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
next-hop-self-rr	Enable/disable setting nexthop's address to interface's IPv4 address for route-reflector routes.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
next-hop-self-rr6	Enable/disable setting nexthop's address to interface's IPv6 address for route-reflector routes.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
override-capability	Enable/disable override result of capability negotiation.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

Parameter	Description	Type	Size	Default						
passive	Enable/disable sending of open messages to this neighbor.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
remove-private-as	Enable/disable remove private AS number from IPv4 outbound updates.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
remove-private-as6	Enable/disable remove private AS number from IPv6 outbound updates.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
route-reflector-client	Enable/disable IPv4 AS route reflector client.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
route-reflector-client6	Enable/disable IPv6 AS route reflector client.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
route-server-client	Enable/disable IPv4 AS route server client.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									

Parameter	Description	Type	Size	Default						
route-server-client6	Enable/disable IPv6 AS route server client.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
shutdown	Enable/disable shutdown this neighbor.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
soft-reconfiguration	Enable/disable allow IPv4 inbound soft reconfiguration.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
soft-reconfiguration6	Enable/disable allow IPv6 inbound soft reconfiguration.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
as-override	Enable/disable replace peer AS with own AS for IPv4.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
as-override6	Enable/disable replace peer AS with own AS for IPv6.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									

Parameter	Description	Type	Size	Default						
strict-capability-match	Enable/disable strict capability matching.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
	Option	Description								
	<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.									
default-originate-routemap	Route map to specify criteria to originate IPv4 default.	string	Maximum length: 35							
default-originate-routemap6	Route map to specify criteria to originate IPv6 default.	string	Maximum length: 35							
description	Description.	string	Maximum length: 63							
distribute-list-in	Filter for IPv4 updates from this neighbor.	string	Maximum length: 35							
distribute-list-in6	Filter for IPv6 updates from this neighbor.	string	Maximum length: 35							
distribute-list-out	Filter for IPv4 updates to this neighbor.	string	Maximum length: 35							
distribute-list-out6	Filter for IPv6 updates to this neighbor.	string	Maximum length: 35							
ebgp-multihop-ttl	EBGP multihop TTL for this peer.	integer	Minimum value: 1 Maximum value: 255	255						
filter-list-in	BGP filter for IPv4 inbound routes.	string	Maximum length: 35							
filter-list-in6	BGP filter for IPv6 inbound routes.	string	Maximum length: 35							
filter-list-out	BGP filter for IPv4 outbound routes.	string	Maximum length: 35							
filter-list-out6	BGP filter for IPv6 outbound routes.	string	Maximum length: 35							
interface	Specify outgoing interface for peer connection. For IPv6 peer, the interface should have link-local address.	string	Maximum length: 15							

Parameter	Description	Type	Size	Default
maximum-prefix	Maximum number of IPv4 prefixes to accept from this peer.	integer	Minimum value: 1 Maximum value: 4294967295	0
maximum-prefix6	Maximum number of IPv6 prefixes to accept from this peer.	integer	Minimum value: 1 Maximum value: 4294967295	0
maximum-prefix-threshold	Maximum IPv4 prefix threshold value.	integer	Minimum value: 1 Maximum value: 100	75
maximum-prefix-threshold6	Maximum IPv6 prefix threshold value.	integer	Minimum value: 1 Maximum value: 100	75
maximum-prefix-warning-only	Enable/disable IPv4 Only give warning message when limit is exceeded.	option	-	disable
	Option	Description		
	enable	Enable setting.		
	disable	Disable setting.		
maximum-prefix-warning-only6	Enable/disable IPv6 Only give warning message when limit is exceeded.	option	-	disable
	Option	Description		
	enable	Enable setting.		
	disable	Disable setting.		
prefix-list-in	IPv4 Inbound filter for updates from this neighbor.	string	Maximum length: 35	
prefix-list-in6	IPv6 Inbound filter for updates from this neighbor.	string	Maximum length: 35	
prefix-list-out	IPv4 Outbound filter for updates to this neighbor.	string	Maximum length: 35	
prefix-list-out6	IPv6 Outbound filter for updates to this neighbor.	string	Maximum length: 35	

Parameter	Description	Type	Size	Default						
remote-as	AS number of neighbor.	integer	Minimum value: 1 Maximum value: 4294967295	0						
local-as	Local AS number of neighbor.	integer	Minimum value: 0 Maximum value: 4294967295	0						
local-as-no-prepend	Do not prepend local-as to incoming updates.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>				Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.
	Option	Description								
	<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.									
local-as-replace-as	Replace real AS with local-as in outgoing updates.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>				Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.
	Option	Description								
	<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.									
retain-stale-time	Time to retain stale routes.	integer	Minimum value: 0 Maximum value: 65535	0						
route-map-in	IPv4 Inbound route map filter.	string	Maximum length: 35							
route-map-in6	IPv6 Inbound route map filter.	string	Maximum length: 35							
route-map-out	IPv4 outbound route map filter.	string	Maximum length: 35							
route-map-out-preferable	IPv4 outbound route map filter if the peer is preferred.	string	Maximum length: 35							
route-map-out6	IPv6 Outbound route map filter.	string	Maximum length: 35							
route-map-out6-preferable	IPv6 outbound route map filter if the peer is preferred.	string	Maximum length: 35							



Parameter	Description	Type	Size	Default										
send-community	IPv4 Send community attribute to neighbor.	option	-	both										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>standard</i></td><td>Standard.</td></tr><tr><td><i>extended</i></td><td>Extended.</td></tr><tr><td><i>both</i></td><td>Both.</td></tr><tr><td><i>disable</i></td><td>Disable</td></tr></table>	Option	Description	<i>standard</i>	Standard.	<i>extended</i>	Extended.	<i>both</i>	Both.	<i>disable</i>	Disable			
	Option	Description												
	<i>standard</i>	Standard.												
	<i>extended</i>	Extended.												
	<i>both</i>	Both.												
	<i>disable</i>	Disable												
send-community6	IPv6 Send community attribute to neighbor.	option	-	both										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>standard</i></td><td>Standard.</td></tr><tr><td><i>extended</i></td><td>Extended.</td></tr><tr><td><i>both</i></td><td>Both.</td></tr><tr><td><i>disable</i></td><td>Disable</td></tr></table>	Option	Description	<i>standard</i>	Standard.	<i>extended</i>	Extended.	<i>both</i>	Both.	<i>disable</i>	Disable			
	Option	Description												
	<i>standard</i>	Standard.												
	<i>extended</i>	Extended.												
	<i>both</i>	Both.												
	<i>disable</i>	Disable												
keep-alive-timer	Keep alive timer interval (sec).	integer	Minimum value: 0 Maximum value: 65535	4294967295										
holdtime-timer	Interval (sec) before peer considered dead.	integer	Minimum value: 3 Maximum value: 65535	4294967295										
connect-timer	Interval (sec) for connect timer.	integer	Minimum value: 0 Maximum value: 65535	4294967295										
unsuppress-map	IPv4 Route map to selectively unsuppress suppressed routes.	string	Maximum length: 35											
unsuppress-map6	IPv6 Route map to selectively unsuppress suppressed routes.	string	Maximum length: 35											
update-source	Interface to use as source IP/IPv6 address of TCP connections.	string	Maximum length: 15											
weight	Neighbor weight.	integer	Minimum value: 0 Maximum value: 65535	4294967295										

Parameter	Description	Type	Size	Default										
restart-time	Graceful restart delay time.	integer	Minimum value: 0 Maximum value: 3600	0										
additional-path	Enable/disable IPv4 additional-path capability.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>send</i></td><td>Enable sending additional paths.</td></tr><tr><td><i>receive</i></td><td>Enable receiving additional paths.</td></tr><tr><td><i>both</i></td><td>Enable sending and receiving additional paths.</td></tr><tr><td><i>disable</i></td><td>Disable additional paths.</td></tr></table>	Option	Description	<i>send</i>	Enable sending additional paths.	<i>receive</i>	Enable receiving additional paths.	<i>both</i>	Enable sending and receiving additional paths.	<i>disable</i>	Disable additional paths.			
	Option	Description												
	<i>send</i>	Enable sending additional paths.												
	<i>receive</i>	Enable receiving additional paths.												
	<i>both</i>	Enable sending and receiving additional paths.												
<i>disable</i>	Disable additional paths.													
additional-path6	Enable/disable IPv6 additional-path capability.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>send</i></td><td>Enable sending additional paths.</td></tr><tr><td><i>receive</i></td><td>Enable receiving additional paths.</td></tr><tr><td><i>both</i></td><td>Enable sending and receiving additional paths.</td></tr><tr><td><i>disable</i></td><td>Disable additional paths.</td></tr></table>	Option	Description	<i>send</i>	Enable sending additional paths.	<i>receive</i>	Enable receiving additional paths.	<i>both</i>	Enable sending and receiving additional paths.	<i>disable</i>	Disable additional paths.			
	Option	Description												
	<i>send</i>	Enable sending additional paths.												
	<i>receive</i>	Enable receiving additional paths.												
	<i>both</i>	Enable sending and receiving additional paths.												
<i>disable</i>	Disable additional paths.													
adv-additional-path	Number of IPv4 additional paths that can be advertised to this neighbor.	integer	Minimum value: 2 Maximum value: 255	2										
adv-additional-path6	Number of IPv6 additional paths that can be advertised to this neighbor.	integer	Minimum value: 2 Maximum value: 255	2										

### config neighbor-range

Parameter	Description	Type	Size	Default
id	Neighbor range ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
prefix	Neighbor range prefix.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0

Parameter	Description	Type	Size	Default
max-neighbor-num	Maximum number of neighbors.	integer	Minimum value: 1 Maximum value: 1000	0
neighbor-group	Neighbor group name.	string	Maximum length: 63	

### config neighbor-range6

Parameter	Description	Type	Size	Default
id	IPv6 neighbor range ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
prefix6	IPv6 prefix.	ipv6-network	Not Specified	::/0
max-neighbor-num	Maximum number of neighbors.	integer	Minimum value: 1 Maximum value: 1000	0
neighbor-group	Neighbor group name.	string	Maximum length: 63	

### config network

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
prefix	Network prefix.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0
network-import-check	Configure insurance of BGP network route existence in IGP.	option	-	global
		Option	Description	
		<i>global</i>	Use global network sync value.	

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable network sync per prefix.		
	<i>disable</i>	Disable network sync per prefix.		
backdoor	Enable/disable route as backdoor.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
route-map	Route map to modify generated route.	string	Maximum length: 35	

## config network6

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
prefix6	Network IPv6 prefix.	ipv6-network	Not Specified	::/0
network-import-check	Configure insurance of BGP network route existence in IGP.	option	-	global
	<b>Option</b>	<b>Description</b>		
	<i>global</i>	Use global network sync value.		
	<i>enable</i>	Enable network sync per prefix.		
	<i>disable</i>	Disable network sync per prefix.		
backdoor	Enable/disable route as backdoor.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
route-map	Route map to modify generated route.	string	Maximum length: 35	

## config redistribute

Parameter	Description	Type	Size	Default
name	Distribute list entry name.	string	Maximum length: 35	
status	Status.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
route-map	Route map name.	string	Maximum length: 35	

## config redistribute6

Parameter	Description	Type	Size	Default
name	Distribute list entry name.	string	Maximum length: 35	
status	Status.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
route-map	Route map name.	string	Maximum length: 35	

## config vrf-leak

Parameter	Description	Type	Size	Default
vrf	Origin VRF ID.	string	Maximum length: 7	

## config target

Parameter	Description	Type	Size	Default
vrf	Target VRF ID.	string	Maximum length: 7	
route-map	Route map of VRF leaking.	string	Maximum length: 35	

Parameter	Description	Type	Size	Default
interface	Interface which is used to leak routes to target VRF.	string	Maximum length: 15	

### config vrf-leak6

Parameter	Description	Type	Size	Default
vrf	Origin VRF ID.	string	Maximum length: 7	

### config target

Parameter	Description	Type	Size	Default
vrf	Target VRF ID.	string	Maximum length: 7	
route-map	Route map of VRF leaking.	string	Maximum length: 35	
interface	Interface which is used to leak routes to target VRF.	string	Maximum length: 15	

## config router community-list

Configure community lists.

```

config router community-list
  Description: Configure community lists.
  edit <name>
    config rule
      Description: Community list rule.
      edit <id>
        set action [deny|permit]
        set regexp {string}
        set match {string}
      next
    end
    set type [standard|expanded]
  next
end

```

### config router community-list

Parameter	Description	Type	Size	Default
name	Community list name.	string	Maximum length: 35	

Parameter	Description	Type	Size	Default
type	Community list type (standard or expanded).	option	-	standard
	<b>Option</b>	<b>Description</b>		
	<i>standard</i>	Standard community list type.		
	<i>expanded</i>	Expanded community list type.		

## config rule

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
action	Permit or deny route-based operations, based on the route's COMMUNITY attribute.	option	-	
	<b>Option</b>	<b>Description</b>		
	<i>deny</i>	Deny route-based operations.		
	<i>permit</i>	Permit or allow route-based operations.		
regex	Ordered list of COMMUNITY attributes as a regular expression.	string	Maximum length: 255	
match	Community specifications for matching a reserved community.	string	Maximum length: 255	

## config router isis

Configure IS-IS.

```
config router isis
  Description: Configure IS-IS.
  set adjacency-check [enable|disable]
  set adjacency-check6 [enable|disable]
  set adv-passive-only [enable|disable]
  set adv-passive-only6 [enable|disable]
  set auth-keychain-l1 {string}
  set auth-keychain-l2 {string}
  set auth-mode-l1 [password|md5]
  set auth-mode-l2 [password|md5]
  set auth-password-l1 {password}
  set auth-password-l2 {password}
  set auth-sendonly-l1 [enable|disable]
  set auth-sendonly-l2 [enable|disable]
```

```

set default-originate [enable|disable]
set default-originate6 [enable|disable]
set dynamic-hostname [enable|disable]
set ignore-lsp-errors [enable|disable]
set is-type [level-1-2|level-1|...]
config isis-interface
    Description: IS-IS interface configuration.
    edit <name>
        set status [enable|disable]
        set status6 [enable|disable]
        set network-type [broadcast|point-to-point|...]
        set circuit-type [level-1-2|level-1|...]
        set csnp-interval-l1 {integer}
        set csnp-interval-l2 {integer}
        set hello-interval-l1 {integer}
        set hello-interval-l2 {integer}
        set hello-multiplier-l1 {integer}
        set hello-multiplier-l2 {integer}
        set hello-padding [enable|disable]
        set lsp-interval {integer}
        set lsp-retransmit-interval {integer}
        set metric-l1 {integer}
        set metric-l2 {integer}
        set wide-metric-l1 {integer}
        set wide-metric-l2 {integer}
        set auth-password-l1 {password}
        set auth-password-l2 {password}
        set auth-keychain-l1 {string}
        set auth-keychain-l2 {string}
        set auth-send-only-l1 [enable|disable]
        set auth-send-only-l2 [enable|disable]
        set auth-mode-l1 [md5|password]
        set auth-mode-l2 [md5|password]
        set priority-l1 {integer}
        set priority-l2 {integer}
        set mesh-group [enable|disable]
        set mesh-group-id {integer}
    next
end
config isis-net
    Description: IS-IS net configuration.
    edit <id>
        set net {user}
    next
end
set lsp-gen-interval-l1 {integer}
set lsp-gen-interval-l2 {integer}
set lsp-refresh-interval {integer}
set max-lsp-lifetime {integer}
set metric-style [narrow|wide|...]
set overload-bit [enable|disable]
set overload-bit-on-startup {integer}
set overload-bit-suppress {option1}, {option2}, ...
config redistribute
    Description: IS-IS redistribute protocols.
    edit <protocol>

```



```

        set status [enable|disable]
        set metric {integer}
        set metric-type [external|internal]
        set level [level-1-2|level-1|...]
        set routemap {string}
    next
end
set redistribute-l1 [enable|disable]
set redistribute-l1-list {string}
set redistribute-l2 [enable|disable]
set redistribute-l2-list {string}
config redistribute6
    Description: IS-IS IPv6 redistribution for routing protocols.
    edit <protocol>
        set status [enable|disable]
        set metric {integer}
        set metric-type [external|internal]
        set level [level-1-2|level-1|...]
        set routemap {string}
    next
end
set redistribute6-l1 [enable|disable]
set redistribute6-l1-list {string}
set redistribute6-l2 [enable|disable]
set redistribute6-l2-list {string}
set spf-interval-exp-l1 {user}
set spf-interval-exp-l2 {user}
config summary-address
    Description: IS-IS summary addresses.
    edit <id>
        set prefix {ipv4-classnet-any}
        set level [level-1-2|level-1|...]
    next
end
config summary-address6
    Description: IS-IS IPv6 summary address.
    edit <id>
        set prefix6 {ipv6-prefix}
        set level [level-1-2|level-1|...]
    next
end
end

```

## config router isis

Parameter	Description	Type	Size	Default
adjacency-check	Enable/disable adjacency check.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable adjacency check.		

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable adjacency check.		
adjacency-check6	Enable/disable IPv6 adjacency check.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable IPv6 adjacency check.		
	<i>disable</i>	Disable IPv6 adjacency check.		
adv-passive-only	Enable/disable IS-IS advertisement of passive interfaces only.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Advertise passive interfaces only.		
	<i>disable</i>	Advertise all IS-IS enabled interfaces.		
adv-passive-only6	Enable/disable IPv6 IS-IS advertisement of passive interfaces only.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Advertise passive interfaces only.		
	<i>disable</i>	Advertise all IS-IS enabled interfaces.		
auth-keychain-l1	Authentication key-chain for level 1 PDUs.	string	Maximum length: 35	
auth-keychain-l2	Authentication key-chain for level 2 PDUs.	string	Maximum length: 35	
auth-mode-l1	Level 1 authentication mode.	option	-	password
	<b>Option</b>	<b>Description</b>		
	<i>password</i>	Password.		
	<i>md5</i>	MD5.		
auth-mode-l2	Level 2 authentication mode.	option	-	password
	<b>Option</b>	<b>Description</b>		
	<i>password</i>	Password.		
	<i>md5</i>	MD5.		

Parameter	Description	Type	Size	Default						
auth-password-l1	Authentication password for level 1 PDUs.	password	Not Specified							
auth-password-l2	Authentication password for level 2 PDUs.	password	Not Specified							
auth-sendonly-l1	Enable/disable level 1 authentication send-only.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable level 1 authentication send-only.</td></tr><tr><td><i>disable</i></td><td>Disable level 1 authentication send-only.</td></tr></table>	Option	Description	<i>enable</i>	Enable level 1 authentication send-only.	<i>disable</i>	Disable level 1 authentication send-only.			
Option	Description									
<i>enable</i>	Enable level 1 authentication send-only.									
<i>disable</i>	Disable level 1 authentication send-only.									
auth-sendonly-l2	Enable/disable level 2 authentication send-only.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable level 2 authentication send-only.</td></tr><tr><td><i>disable</i></td><td>Disable level 2 authentication send-only.</td></tr></table>	Option	Description	<i>enable</i>	Enable level 2 authentication send-only.	<i>disable</i>	Disable level 2 authentication send-only.			
Option	Description									
<i>enable</i>	Enable level 2 authentication send-only.									
<i>disable</i>	Disable level 2 authentication send-only.									
default-originate	Enable/disable distribution of default route information.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable distribution of default route information.</td></tr><tr><td><i>disable</i></td><td>Disable distribution of default route information.</td></tr></table>	Option	Description	<i>enable</i>	Enable distribution of default route information.	<i>disable</i>	Disable distribution of default route information.			
Option	Description									
<i>enable</i>	Enable distribution of default route information.									
<i>disable</i>	Disable distribution of default route information.									
default-originate6	Enable/disable distribution of default IPv6 route information.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable distribution of default IPv6 route information.</td></tr><tr><td><i>disable</i></td><td>Disable distribution of default IPv6 route information.</td></tr></table>	Option	Description	<i>enable</i>	Enable distribution of default IPv6 route information.	<i>disable</i>	Disable distribution of default IPv6 route information.			
Option	Description									
<i>enable</i>	Enable distribution of default IPv6 route information.									
<i>disable</i>	Disable distribution of default IPv6 route information.									
dynamic-hostname	Enable/disable dynamic hostname.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable dynamic hostname.</td></tr><tr><td><i>disable</i></td><td>Disable dynamic hostname.</td></tr></table>	Option	Description	<i>enable</i>	Enable dynamic hostname.	<i>disable</i>	Disable dynamic hostname.			
Option	Description									
<i>enable</i>	Enable dynamic hostname.									
<i>disable</i>	Disable dynamic hostname.									
ignore-lsp-errors	Enable/disable ignoring of LSP errors with bad checksums.	option	-	disable						

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable ignoring of LSP errors with bad checksums.		
	<i>disable</i>	Disable ignoring of LSP errors with bad checksums.		
is-type	IS type.	option	-	level-1-2
	<b>Option</b>	<b>Description</b>		
	<i>level-1-2</i>	Level 1 and 2.		
	<i>level-1</i>	Level 1 only.		
	<i>level-2-only</i>	Level 2 only.		
lsp-gen-interval-l1	Minimum interval for level 1 LSP regenerating.	integer	Minimum value: 1 Maximum value: 120	30
lsp-gen-interval-l2	Minimum interval for level 2 LSP regenerating.	integer	Minimum value: 1 Maximum value: 120	30
lsp-refresh-interval	LSP refresh time in seconds.	integer	Minimum value: 1 Maximum value: 65535	900
max-lsp-lifetime	Maximum LSP lifetime in seconds.	integer	Minimum value: 350 Maximum value: 65535	1200
metric-style	Use old-style (ISO 10589) or new-style packet formats.	option	-	narrow
	<b>Option</b>	<b>Description</b>		
	<i>narrow</i>	Use old style of TLVs with narrow metric.		
	<i>wide</i>	Use new style of TLVs to carry wider metric.		
	<i>transition</i>	Send and accept both styles of TLVs during transition.		
	<i>narrow-transition</i>	Narrow and accept both styles of TLVs during transition.		

Parameter	Description	Type	Size	Default																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>narrow-transition-l1</i></td><td>Narrow-transition level-1 only.</td></tr><tr><td><i>narrow-transition-l2</i></td><td>Narrow-transition level-2 only.</td></tr><tr><td><i>wide-l1</i></td><td>Wide level-1 only.</td></tr><tr><td><i>wide-l2</i></td><td>Wide level-2 only.</td></tr><tr><td><i>wide-transition</i></td><td>Wide and accept both styles of TLVs during transition.</td></tr><tr><td><i>wide-transition-l1</i></td><td>Wide-transition level-1 only.</td></tr><tr><td><i>wide-transition-l2</i></td><td>Wide-transition level-2 only.</td></tr><tr><td><i>transition-l1</i></td><td>Transition level-1 only.</td></tr><tr><td><i>transition-l2</i></td><td>Transition level-2 only.</td></tr></table>	Option	Description	<i>narrow-transition-l1</i>	Narrow-transition level-1 only.	<i>narrow-transition-l2</i>	Narrow-transition level-2 only.	<i>wide-l1</i>	Wide level-1 only.	<i>wide-l2</i>	Wide level-2 only.	<i>wide-transition</i>	Wide and accept both styles of TLVs during transition.	<i>wide-transition-l1</i>	Wide-transition level-1 only.	<i>wide-transition-l2</i>	Wide-transition level-2 only.	<i>transition-l1</i>	Transition level-1 only.	<i>transition-l2</i>	Transition level-2 only.			
	Option	Description																						
	<i>narrow-transition-l1</i>	Narrow-transition level-1 only.																						
	<i>narrow-transition-l2</i>	Narrow-transition level-2 only.																						
	<i>wide-l1</i>	Wide level-1 only.																						
	<i>wide-l2</i>	Wide level-2 only.																						
	<i>wide-transition</i>	Wide and accept both styles of TLVs during transition.																						
	<i>wide-transition-l1</i>	Wide-transition level-1 only.																						
	<i>wide-transition-l2</i>	Wide-transition level-2 only.																						
	<i>transition-l1</i>	Transition level-1 only.																						
<i>transition-l2</i>	Transition level-2 only.																							
overload-bit	Enable/disable signal other routers not to use us in SPF.	option	-	disable																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable overload bit.</td></tr><tr><td><i>disable</i></td><td>Disable overload bit.</td></tr></table>	Option	Description	<i>enable</i>	Enable overload bit.	<i>disable</i>	Disable overload bit.																	
	Option	Description																						
	<i>enable</i>	Enable overload bit.																						
<i>disable</i>	Disable overload bit.																							
overload-bit-on-startup	Overload-bit only temporarily after reboot.	integer	Minimum value: 5 Maximum value: 86400	0																				
overload-bit-suppress	Suppress overload-bit for the specific prefixes.	option	-																					
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>external</i></td><td>External.</td></tr><tr><td><i>interlevel</i></td><td>Inter-level.</td></tr></table>	Option	Description	<i>external</i>	External.	<i>interlevel</i>	Inter-level.																	
	Option	Description																						
	<i>external</i>	External.																						
<i>interlevel</i>	Inter-level.																							
redistribute-l1	Enable/disable redistribution of level 1 routes into level 2.	option	-	disable																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable redistribution of level 1 routes into level 2.</td></tr><tr><td><i>disable</i></td><td>Disable redistribution of level 1 routes into level 2.</td></tr></table>	Option	Description	<i>enable</i>	Enable redistribution of level 1 routes into level 2.	<i>disable</i>	Disable redistribution of level 1 routes into level 2.																	
	Option	Description																						
	<i>enable</i>	Enable redistribution of level 1 routes into level 2.																						
<i>disable</i>	Disable redistribution of level 1 routes into level 2.																							

Parameter	Description	Type	Size	Default
redistribute-l1-list	Access-list for route redistribution from I1 to I2.	string	Maximum length: 35	
redistribute-l2	Enable/disable redistribution of level 2 routes into level 1.	option	-	disable
	<b>Option</b>		<b>Description</b>	
	<i>enable</i>		Enable redistribution of level 2 routes into level 1.	
	<i>disable</i>		Disable redistribution of level 2 routes into level 1.	
redistribute-l2-list	Access-list for route redistribution from I2 to I1.	string	Maximum length: 35	
redistribute6-l1	Enable/disable redistribution of level 1 IPv6 routes into level 2.	option	-	disable
	<b>Option</b>		<b>Description</b>	
	<i>enable</i>		Enable redistribution of level 1 IPv6 routes into level 2.	
	<i>disable</i>		Disable redistribution of level 1 IPv6 routes into level 2.	
redistribute6-l1-list	Access-list for IPv6 route redistribution from I1 to I2.	string	Maximum length: 35	
redistribute6-l2	Enable/disable redistribution of level 2 IPv6 routes into level 1.	option	-	disable
	<b>Option</b>		<b>Description</b>	
	<i>enable</i>		Enable redistribution of level 2 IPv6 routes into level 1.	
	<i>disable</i>		Disable redistribution of level 2 IPv6 routes into level 1.	
redistribute6-l2-list	Access-list for IPv6 route redistribution from I2 to I1.	string	Maximum length: 35	
spf-interval-exp-l1	Level 1 SPF calculation delay.	user	Not Specified	
spf-interval-exp-l2	Level 2 SPF calculation delay.	user	Not Specified	

## config isis-interface

Parameter	Description	Type	Size	Default
name	IS-IS interface name.	string	Maximum length: 15	
status	Enable/disable interface for IS-IS.	option	-	disable

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable interface for IS-IS.		
	<i>disable</i>	Disable interface for IS-IS.		
status6	Enable/disable IPv6 interface for IS-IS.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable IPv6 interface for IS-IS.		
	<i>disable</i>	Disable IPv6 interface for IS-IS.		
network-type	IS-IS interface's network type.	option	-	
	<b>Option</b>	<b>Description</b>		
	<i>broadcast</i>	Broadcast.		
	<i>point-to-point</i>	Point-to-point.		
	<i>loopback</i>	Loopback.		
circuit-type	IS-IS interface's circuit type.	option	-	level-1-2
	<b>Option</b>	<b>Description</b>		
	<i>level-1-2</i>	Level 1 and 2.		
	<i>level-1</i>	Level 1.		
	<i>level-2</i>	Level 2.		
csnp-interval- l1	Level 1 CSNP interval.	integer	Minimum value: 1 Maximum value: 65535	10
csnp-interval- l2	Level 2 CSNP interval.	integer	Minimum value: 1 Maximum value: 65535	10
hello-interval- l1	Level 1 hello interval.	integer	Minimum value: 0 Maximum value: 65535	10
hello-interval- l2	Level 2 hello interval.	integer	Minimum value: 0 Maximum value: 65535	10

Parameter	Description	Type	Size	Default						
hello-multiplier-l1	Level 1 multiplier for Hello holding time.	integer	Minimum value: 2 Maximum value: 100	3						
hello-multiplier-l2	Level 2 multiplier for Hello holding time.	integer	Minimum value: 2 Maximum value: 100	3						
hello-padding	Enable/disable padding to IS-IS hello packets.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable padding to IS-IS hello packets.</td></tr><tr><td><i>disable</i></td><td>Disable padding to IS-IS hello packets.</td></tr></table>				Option	Description	<i>enable</i>	Enable padding to IS-IS hello packets.	<i>disable</i>	Disable padding to IS-IS hello packets.
	Option	Description								
	<i>enable</i>	Enable padding to IS-IS hello packets.								
<i>disable</i>	Disable padding to IS-IS hello packets.									
lsp-interval	LSP transmission interval (milliseconds).	integer	Minimum value: 1 Maximum value: 4294967295	33						
lsp-retransmit-interval	LSP retransmission interval (sec).	integer	Minimum value: 1 Maximum value: 65535	5						
metric-l1	Level 1 metric for interface.	integer	Minimum value: 1 Maximum value: 63	10						
metric-l2	Level 2 metric for interface.	integer	Minimum value: 1 Maximum value: 63	10						
wide-metric-l1	Level 1 wide metric for interface.	integer	Minimum value: 1 Maximum value: 16777214	10						
wide-metric-l2	Level 2 wide metric for interface.	integer	Minimum value: 1 Maximum value: 16777214	10						



Parameter	Description	Type	Size	Default
auth-password-l1	Authentication password for level 1 PDUs.	password	Not Specified	
auth-password-l2	Authentication password for level 2 PDUs.	password	Not Specified	
auth-keychain-l1	Authentication key-chain for level 1 PDUs.	string	Maximum length: 35	
auth-keychain-l2	Authentication key-chain for level 2 PDUs.	string	Maximum length: 35	
auth-send-only-l1	Enable/disable authentication send-only for level 1 PDUs.	option	-	disable
	<b>Option</b>		<b>Description</b>	
	<i>enable</i>		Enable authentication send-only for level 1 PDUs.	
	<i>disable</i>		Disable authentication send-only for level 1 PDUs.	
auth-send-only-l2	Enable/disable authentication send-only for level 2 PDUs.	option	-	disable
	<b>Option</b>		<b>Description</b>	
	<i>enable</i>		Enable authentication send-only for level 2 PDUs.	
	<i>disable</i>		Disable authentication send-only for level 2 PDUs.	
auth-mode-l1	Level 1 authentication mode.	option	-	password
	<b>Option</b>		<b>Description</b>	
	<i>md5</i>		MD5.	
	<i>password</i>		Password.	
auth-mode-l2	Level 2 authentication mode.	option	-	password
	<b>Option</b>		<b>Description</b>	
	<i>md5</i>		MD5.	
	<i>password</i>		Password.	
priority-l1	Level 1 priority.	integer	Minimum value: 0 Maximum value: 127	64

Parameter	Description	Type	Size	Default
priority-l2	Level 2 priority.	integer	Minimum value: 0 Maximum value: 127	64
mesh-group	Enable/disable IS-IS mesh group.	option	-	disable
	Option	Description		
	enable	Enable IS-IS mesh group.		
	disable	Disable IS-IS mesh group.		
mesh-group-id	Mesh group ID <0-4294967295>, 0: mesh-group blocked.	integer	Minimum value: 0 Maximum value: 4294967295	0

### config isis-net

Parameter	Description	Type	Size	Default
id	ISIS network ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
net	IS-IS networks (format = xx.xxxx. .xxxx.xx.).	user	Not Specified	

### config redistribute

Parameter	Description	Type	Size	Default
protocol	Protocol name.	string	Maximum length: 35	
status	Status.	option	-	disable
	Option	Description		
	enable	Enable.		
	disable	Disable.		

Parameter	Description	Type	Size	Default
metric	Metric.	integer	Minimum value: 0 Maximum value: 4261412864	0
metric-type	Metric type.	option	-	internal
	<b>Option</b> <b>Description</b>			
	<i>external</i>	External.		
	<i>internal</i>	Internal.		
level	Level.	option	-	level-2
	<b>Option</b> <b>Description</b>			
	<i>level-1-2</i>	Level 1 and 2.		
	<i>level-1</i>	Level 1.		
	<i>level-2</i>	Level 2.		
routemap	Route map name.	string	Maximum length: 35	

## config redistribute6

Parameter	Description	Type	Size	Default
protocol	Protocol name.	string	Maximum length: 35	
status	Enable/disable redistribution.	option	-	disable
	Option	Description		
	enable	Enable redistribution.		
	disable	Disable redistribution.		
metric	Metric.	integer	Minimum value: 0 Maximum value: 4261412864	0
metric-type	Metric type.	option	-	internal

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>external</i>	External metric type.		
	<i>internal</i>	Internal metric type.		
level	Level.	option	-	level-2
	<b>Option</b>	<b>Description</b>		
	<i>level-1-2</i>	Level 1 and 2.		
	<i>level-1</i>	Level 1.		
	<i>level-2</i>	Level 2.		
routemap	Route map name.	string	Maximum length: 35	

### config summary-address

Parameter	Description	Type	Size	Default
id	Summary address entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
prefix	Prefix.	ipv4-classnet-any	Not Specified	0.0.0.0 0.0.0.0
level	Level.	option	-	level-2
	<b>Option</b>	<b>Description</b>		
	<i>level-1-2</i>	Level 1 and 2.		
	<i>level-1</i>	Level 1.		
	<i>level-2</i>	Level 2.		

## config summary-address6

Parameter	Description	Type	Size	Default
id	Prefix entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
prefix6	IPv6 prefix.	ipv6-prefix	Not Specified	::/0
level	Level.	option	-	level-2
		Option	Description	
		level-1-2	Level 1 and 2.	
		level-1	Level 1.	
		level-2	Level 2.	

## config router key-chain

Configure key-chain.

```
config router key-chain
  Description: Configure key-chain.
  edit <name>
    config key
      Description: Configuration method to edit key settings.
      edit <id>
        set accept-lifetime {user}
        set send-lifetime {user}
        set key-string {password}
        set algorithm [md5|hmac-sha1|...]
      next
    end
  next
end
```

## config router key-chain

Parameter	Description	Type	Size	Default
name	Key-chain name.	string	Maximum length: 35	

## config key

Parameter	Description	Type	Size	Default
id	Key ID.	string	Maximum length: 10	
accept-lifetime	Lifetime of received authentication key (format: hh:mm:ss day month year).	user	Not Specified	
send-lifetime	Lifetime of sent authentication key (format: hh:mm:ss day month year).	user	Not Specified	
key-string	Password for the key (maximum = 64 characters).	password	Not Specified	
algorithm	Cryptographic algorithm.	option	-	md5
		Option	Description	
		<i>md5</i>	MD5.	
		<i>hmac-sha1</i>	HMAC-SHA1.	
		<i>hmac-sha256</i>	HMAC-SHA256.	
		<i>hmac-sha384</i>	HMAC-SHA384.	
		<i>hmac-sha512</i>	HMAC-SHA512.	

## config router multicast-flow

Configure multicast-flow.

```
config router multicast-flow
  Description: Configure multicast-flow.
  edit <name>
    set comments {string}
    config flows
      Description: Multicast-flow entries.
      edit <id>
        set group-addr {ipv4-address-any}
        set source-addr {ipv4-address-any}
      next
    end
  next
end
```

## config router multicast-flow

Parameter	Description	Type	Size	Default
comments	Comment.	string	Maximum length: 127	
name	Name.	string	Maximum length: 35	

## config flows

Parameter	Description	Type	Size	Default
id	Flow ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
group-addr	Multicast group IP address.	ipv4-address-any	Not Specified	0.0.0.0
source-addr	Multicast source IP address.	ipv4-address-any	Not Specified	0.0.0.0

## config router multicast

Configure router multicast.

```
config router multicast
  Description: Configure router multicast.
  config interface
    Description: PIM interfaces.
    edit <name>
      set ttl-threshold {integer}
      set pim-mode [sparse-mode|dense-mode]
      set passive [enable|disable]
      set bfd [enable|disable]
      set neighbour-filter {string}
      set hello-interval {integer}
      set hello-holdtime {integer}
      set cisco-exclude-genid [enable|disable]
      set dr-priority {integer}
      set propagation-delay {integer}
      set state-refresh-interval {integer}
      set rp-candidate [enable|disable]
      set rp-candidate-group {string}
      set rp-candidate-priority {integer}
      set rp-candidate-interval {integer}
```

```

    set multicast-flow {string}
    set static-group {string}
    set rpf-nbr-fail-back [enable|disable]
    set rpf-nbr-fail-back-filter {string}
    config join-group
        Description: Join multicast groups.
        edit <address>
            next
        end
    config igmp
        Description: IGMP configuration options.
        set access-group {string}
        set version [3|2|...]
        set immediate-leave-group {string}
        set last-member-query-interval {integer}
        set last-member-query-count {integer}
        set query-max-response-time {integer}
        set query-interval {integer}
        set query-timeout {integer}
        set router-alert-check [enable|disable]
    end
next
end
set multicast-routing [enable|disable]
config pim-sm-global
    Description: PIM sparse-mode global settings.
    set message-interval {integer}
    set join-prune-holdtime {integer}
    set accept-register-list {string}
    set accept-source-list {string}
    set bsr-candidate [enable|disable]
    set bsr-interface {string}
    set bsr-priority {integer}
    set bsr-hash {integer}
    set bsr-allow-quick-refresh [enable|disable]
    set cisco-register-checksum [enable|disable]
    set cisco-register-checksum-group {string}
    set cisco-crp-prefix [enable|disable]
    set cisco-ignore-rp-set-priority [enable|disable]
    set register-rp-reachability [enable|disable]
    set register-source [disable|interface|...]
    set register-source-interface {string}
    set register-source-ip {ipv4-address}
    set register-supression {integer}
    set null-register-retries {integer}
    set rp-register-keepalive {integer}
    set spt-threshold [enable|disable]
    set spt-threshold-group {string}
    set ssm [enable|disable]
    set ssm-range {string}
    set register-rate-limit {integer}
    config rp-address
        Description: Statically configure RP addresses.
        edit <id>
            set ip-address {ipv4-address}
            set group {string}

```



```

        next
    end
end
set route-limit {integer}
set route-threshold {integer}
end

```

## config router multicast

Parameter	Description	Type	Size	Default
multicast-routing	Enable/disable IP multicast routing.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable IP multicast routing.		
	<i>disable</i>	Disable IP multicast routing.		
route-limit	Maximum number of multicast routes.	integer	Minimum value: 1 Maximum value: 2147483647	2147483647
route-threshold	Generate warnings when the number of multicast routes exceeds this number, must not be greater than route-limit.	integer	Minimum value: 1 Maximum value: 2147483647	

## config interface

Parameter	Description	Type	Size	Default						
name	Interface name.	string	Maximum length: 15							
ttl-threshold	Minimum TTL of multicast packets that will be forwarded.	integer	Minimum value: 1 Maximum value: 255	1						
pim-mode	PIM operation mode.	option	-	sparse-mode						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>sparse-mode</td><td>sparse-mode</td></tr><tr><td>dense-mode</td><td>dense-mode</td></tr></table>				Option	Description	sparse-mode	sparse-mode	dense-mode	dense-mode
Option	Description									
sparse-mode	sparse-mode									
dense-mode	dense-mode									

Parameter	Description	Type	Size	Default						
passive	Enable/disable listening to IGMP but not participating in PIM.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Listen only.</td></tr><tr><td><i>disable</i></td><td>Participate in PIM.</td></tr></table>	Option	Description	<i>enable</i>	Listen only.	<i>disable</i>	Participate in PIM.			
Option	Description									
<i>enable</i>	Listen only.									
<i>disable</i>	Participate in PIM.									
bfd	Enable/disable Protocol Independent Multicast (PIM) Bidirectional Forwarding Detection (BFD).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Protocol Independent Multicast (PIM) Bidirectional Forwarding Detection (BFD).</td></tr><tr><td><i>disable</i></td><td>Disable Protocol Independent Multicast (PIM) Bidirectional Forwarding Detection (BFD).</td></tr></table>	Option	Description	<i>enable</i>	Enable Protocol Independent Multicast (PIM) Bidirectional Forwarding Detection (BFD).	<i>disable</i>	Disable Protocol Independent Multicast (PIM) Bidirectional Forwarding Detection (BFD).			
Option	Description									
<i>enable</i>	Enable Protocol Independent Multicast (PIM) Bidirectional Forwarding Detection (BFD).									
<i>disable</i>	Disable Protocol Independent Multicast (PIM) Bidirectional Forwarding Detection (BFD).									
neighbour-filter	Routers acknowledged as neighbor routers.	string	Maximum length: 35							
hello-interval	Interval between sending PIM hello messages.	integer	Minimum value: 1 Maximum value: 65535	30						
hello-holdtime	Time before old neighbor information expires.	integer	Minimum value: 1 Maximum value: 65535							
cisco-exclude-genid	Exclude GenID from hello packets (compatibility with old Cisco IOS).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Do not send GenID.</td></tr><tr><td><i>disable</i></td><td>Send GenID according to standard.</td></tr></table>	Option	Description	<i>enable</i>	Do not send GenID.	<i>disable</i>	Send GenID according to standard.			
Option	Description									
<i>enable</i>	Do not send GenID.									
<i>disable</i>	Send GenID according to standard.									
dr-priority	DR election priority.	integer	Minimum value: 1 Maximum value: 4294967295	1						
propagation-delay	Delay flooding packets on this interface.	integer	Minimum value: 100 Maximum value: 5000	500						

Parameter	Description	Type	Size	Default						
state-refresh-interval	Interval between sending state-refresh packets.	integer	Minimum value: 1 Maximum value: 100	60						
rp-candidate	Enable/disable compete to become RP in elections.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Compete for RP elections.</td></tr><tr><td><i>disable</i></td><td>Do not compete for RP elections.</td></tr></table>	Option	Description	<i>enable</i>	Compete for RP elections.	<i>disable</i>	Do not compete for RP elections.			
Option	Description									
<i>enable</i>	Compete for RP elections.									
<i>disable</i>	Do not compete for RP elections.									
rp-candidate-group	Multicast groups managed by this RP.	string	Maximum length: 35							
rp-candidate-priority	Router's priority as RP.	integer	Minimum value: 0 Maximum value: 255	192						
rp-candidate-interval	RP candidate advertisement interval.	integer	Minimum value: 1 Maximum value: 16383	60						
multicast-flow	Acceptable source for multicast group.	string	Maximum length: 35							
static-group	Statically set multicast groups to forward out.	string	Maximum length: 35							
rpf-nbr-fail-back	Enable/disable fail back for RPF neighbor query.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable fail back for RPF neighbor query.</td></tr><tr><td><i>disable</i></td><td>Disable fail back for RPF neighbor query.</td></tr></table>	Option	Description	<i>enable</i>	Enable fail back for RPF neighbor query.	<i>disable</i>	Disable fail back for RPF neighbor query.			
Option	Description									
<i>enable</i>	Enable fail back for RPF neighbor query.									
<i>disable</i>	Disable fail back for RPF neighbor query.									
rpf-nbr-fail-back-filter	Filter for fail back RPF neighbors.	string	Maximum length: 35							

### config join-group

Parameter	Description	Type	Size	Default
address	Multicast group IP address.	ipv4-address-any	Not Specified	0.0.0.0

## config igmp

Parameter	Description	Type	Size	Default								
access-group	Groups IGMP hosts are allowed to join.	string	Maximum length: 35									
version	Maximum version of IGMP to support.	option	-	3								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>3</td><td>Version 3 and lower.</td></tr><tr><td>2</td><td>Version 2 and lower.</td></tr><tr><td>1</td><td>Version 1.</td></tr></table>	Option	Description	3	Version 3 and lower.	2	Version 2 and lower.	1	Version 1.			
Option	Description											
3	Version 3 and lower.											
2	Version 2 and lower.											
1	Version 1.											
immediate-leave-group	Groups to drop membership for immediately after receiving IGMPv2 leave.	string	Maximum length: 35									
last-member-query-interval	Timeout between IGMPv2 leave and removing group.	integer	Minimum value: 1 Maximum value: 65535	1000								
last-member-query-count	Number of group specific queries before removing group.	integer	Minimum value: 2 Maximum value: 7	2								
query-max-response-time	Maximum time to wait for a IGMP query response.	integer	Minimum value: 1 Maximum value: 25	10								
query-interval	Interval between queries to IGMP hosts.	integer	Minimum value: 1 Maximum value: 65535	125								
query-timeout	Timeout between queries before becoming querying unit for network.	integer	Minimum value: 60 Maximum value: 900	255								
router-alert-check	Enable/disable require IGMP packets contain router alert option.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Require Router Alert option in IGMP packets.</td></tr><tr><td>disable</td><td>don't require Router Alert option in IGMP packets</td></tr></table>	Option	Description	enable	Require Router Alert option in IGMP packets.	disable	don't require Router Alert option in IGMP packets					
Option	Description											
enable	Require Router Alert option in IGMP packets.											
disable	don't require Router Alert option in IGMP packets											

## config pim-sm-global

Parameter	Description	Type	Size	Default						
message-interval	Period of time between sending periodic PIM join/prune messages in seconds.	integer	Minimum value: 1 Maximum value: 65535	60						
join-prune-holdtime	Join/prune holdtime.	integer	Minimum value: 1 Maximum value: 65535	210						
accept-register-list	Sources allowed to register packets with this Rendezvous Point (RP).	string	Maximum length: 35							
accept-source-list	Sources allowed to send multicast traffic.	string	Maximum length: 35							
bsr-candidate	Enable/disable allowing this router to become a bootstrap router (BSR).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Allow this router to function as a BSR.</td></tr><tr><td><i>disable</i></td><td>Do not allow this router to function as a BSR.</td></tr></table>				Option	Description	<i>enable</i>	Allow this router to function as a BSR.	<i>disable</i>	Do not allow this router to function as a BSR.
Option	Description									
<i>enable</i>	Allow this router to function as a BSR.									
<i>disable</i>	Do not allow this router to function as a BSR.									
bsr-interface	Interface to advertise as candidate BSR.	string	Maximum length: 15							
bsr-priority	BSR priority.	integer	Minimum value: 0 Maximum value: 255	0						
bsr-hash	BSR hash length.	integer	Minimum value: 0 Maximum value: 32	10						
bsr-allow-quick-refresh	Enable/disable accept BSR quick refresh packets from neighbors.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Allow quick refresh packets.</td></tr><tr><td><i>disable</i></td><td>Do not allow quick refresh packets.</td></tr></table>				Option	Description	<i>enable</i>	Allow quick refresh packets.	<i>disable</i>	Do not allow quick refresh packets.
Option	Description									
<i>enable</i>	Allow quick refresh packets.									
<i>disable</i>	Do not allow quick refresh packets.									
cisco-register-checksum	Checksum entire register packet(for old Cisco IOS compatibility).	option	-	disable						

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	register checksum entire packet.		
	<i>disable</i>	Do not register checksum entire packet.		
cisco-register-checksum-group	Cisco register checksum only these groups.	string	Maximum length: 35	
cisco-crp-prefix	Enable/disable making candidate RP compatible with old Cisco IOS.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Do not allow sending group prefix of zero.		
	<i>disable</i>	Allow sending group prefix of zero.		
cisco-ignore-rp-set-priority	Use only hash for RP selection (compatibility with old Cisco IOS).	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Ignore RP-SET priority value.		
	<i>disable</i>	Do not ignore RP-SET priority value.		
register-rp-reachability	Enable/disable check RP is reachable before registering packets.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Check target RP is unicast reachable before registering.		
	<i>disable</i>	Do not check RP unicast reachability.		
register-source	Override source address in register packets.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Use source address of RPF interface.		
	<i>interface</i>	Use primary IP of an interface.		
	<i>ip-address</i>	Use a local IP address.		
register-source-interface	Override with primary interface address.	string	Maximum length: 15	

Parameter	Description	Type	Size	Default						
register-source-ip	Override with local IP address.	ipv4-address	Not Specified	0.0.0.0						
register-supression	Period of time to honor register-stop message.	integer	Minimum value: 1 Maximum value: 65535	60						
null-register-retries	Maximum retries of null register.	integer	Minimum value: 1 Maximum value: 20	1						
rp-register-keepalive	Timeout for RP receiving data on.	integer	Minimum value: 1 Maximum value: 65535	185						
spt-threshold	Enable/disable switching to source specific trees.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Switch to Source tree when available.</td></tr><tr><td>disable</td><td>Do not switch to Source tree when available.</td></tr></table>				Option	Description	enable	Switch to Source tree when available.	disable	Do not switch to Source tree when available.
Option	Description									
enable	Switch to Source tree when available.									
disable	Do not switch to Source tree when available.									
spt-threshold-group	Groups allowed to switch to source tree.	string	Maximum length: 35							
ssm	Enable/disable source specific multicast.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Allow source specific multicast.</td></tr><tr><td>disable</td><td>Do not allow source specific multicast.</td></tr></table>				Option	Description	enable	Allow source specific multicast.	disable	Do not allow source specific multicast.
Option	Description									
enable	Allow source specific multicast.									
disable	Do not allow source specific multicast.									
ssm-range	Groups allowed to source specific multicast.	string	Maximum length: 35							
register-rate-limit	Limit of packets/sec per source registered through this RP.	integer	Minimum value: 0 Maximum value: 65535	0						

## config rp-address

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
ip-address	RP router address.	ipv4-address	Not Specified	0.0.0.0
group	Groups to use this RP.	string	Maximum length: 35	

## config router multicast6

Configure IPv6 multicast.

```
config router multicast6
  Description: Configure IPv6 multicast.
  config interface
    Description: Protocol Independent Multicast (PIM) interfaces.
    edit <name>
      set hello-interval {integer}
      set hello-holdtime {integer}
    next
  end
  set multicast-pmtu [enable|disable]
  set multicast-routing [enable|disable]
  config pim-sm-global
    Description: PIM sparse-mode global settings.
    set register-rate-limit {integer}
    config rp-address
      Description: Statically configured RP addresses.
      edit <id>
        set ip6-address {ipv6-address}
      next
    end
  end
end
```

## config router multicast6

Parameter	Description	Type	Size	Default
multicast-pmtu	Enable/disable PMTU for IPv6 multicast.	option	-	disable



Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable PMTU for IPv6 multicast.		
	<i>disable</i>	Disable PMTU for IPv6 multicast.		
multicast-routing	Enable/disable IPv6 multicast routing.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable IPv6 multicast routing.		
	<i>disable</i>	Disable IPv6 multicast routing.		

### config interface

Parameter	Description	Type	Size	Default
name	Interface name.	string	Maximum length: 15	
hello-interval	Interval between sending PIM hello messages in seconds.	integer	Minimum value: 1 Maximum value: 65535	30
hello-holdtime	Time before old neighbor information expires in seconds.	integer	Minimum value: 1 Maximum value: 65535	

### config pim-sm-global

Parameter	Description	Type	Size	Default
register-rate-limit	Limit of packets/sec per source registered through this RP (0 means unlimited).	integer	Minimum value: 0 Maximum value: 65535	0

## config rp-address

Parameter	Description	Type	Size	Default
id	ID of the entry.	integer	Minimum value: 0 Maximum value: 4294967295	0
ip6-address	RP router IPv6 address.	ipv6-address	Not Specified	::

## config router ospf

Configure OSPF.

```
config router ospf
  Description: Configure OSPF.
  set abr-type [cisco|ibm|...]
  config area
    Description: OSPF area configuration.
    edit <id>
      set shortcut [disable|enable|...]
      set authentication [none|text|...]
      set default-cost {integer}
      set nssa-translator-role [candidate|never|...]
      set stub-type [no-summary|summary]
      set type [regular|nssa|...]
      set nssa-default-information-originate [enable|always|...]
      set nssa-default-information-originate-metric {integer}
      set nssa-default-information-originate-metric-type [1|2]
      set nssa-redistribution [enable|disable]
      set comments {var-string}
    config range
      Description: OSPF area range configuration.
      edit <id>
        set prefix {ipv4-classnet-any}
        set advertise [disable|enable]
        set substitute {ipv4-classnet-any}
        set substitute-status [enable|disable]
      next
    end
  config virtual-link
    Description: OSPF virtual link configuration.
    edit <name>
      set authentication [none|text|...]
      set authentication-key {password}
      set keychain {string}
      set dead-interval {integer}
      set hello-interval {integer}
      set retransmit-interval {integer}
      set transmit-delay {integer}
      set peer {ipv4-address-any}
```

```

        config md5-keys
            Description: MD5 key.
            edit <id>
                set key-string {password}
            next
        end
    next
end
config filter-list
    Description: OSPF area filter-list configuration.
    edit <id>
        set list {string}
        set direction [in|out]
    next
end
next
end
set auto-cost-ref-bandwidth {integer}
set bfd [enable|disable]
set database-overflow [enable|disable]
set database-overflow-max-lsas {integer}
set database-overflow-time-to-recover {integer}
set default-information-metric {integer}
set default-information-metric-type [1|2]
set default-information-originate [enable|always|...]
set default-information-route-map {string}
set default-metric {integer}
set distance {integer}
set distance-external {integer}
set distance-inter-area {integer}
set distance-intra-area {integer}
config distribute-list
    Description: Distribute list configuration.
    edit <id>
        set access-list {string}
        set protocol [connected|static|...]
    next
end
set distribute-list-in {string}
set distribute-route-map-in {string}
set log-neighbour-changes [enable|disable]
config neighbor
    Description: OSPF neighbor configuration are used when OSPF runs on non-broadcast
media.
    edit <id>
        set ip {ipv4-address}
        set poll-interval {integer}
        set cost {integer}
        set priority {integer}
    next
end
config network
    Description: OSPF network configuration.
    edit <id>
        set prefix {ipv4-classnet}
        set area {ipv4-address-any}

```

```

        set comments {var-string}
    next
end
config ospf-interface
    Description: OSPF interface configuration.
    edit <name>
        set comments {var-string}
        set interface {string}
        set ip {ipv4-address}
        set authentication [none|text|...]
        set authentication-key {password}
        set keychain {string}
        set prefix-length {integer}
        set retransmit-interval {integer}
        set transmit-delay {integer}
        set cost {integer}
        set priority {integer}
        set dead-interval {integer}
        set hello-interval {integer}
        set hello-multiplier {integer}
        set database-filter-out [enable|disable]
        set mtu {integer}
        set mtu-ignore [enable|disable]
        set network-type [broadcast|non-broadcast|...]
        set bfd [global|enable|...]
        set status [disable|enable]
        set resync-timeout {integer}
        config md5-keys
            Description: MD5 key.
            edit <id>
                set key-string {password}
            next
        end
    next
end
set passive-interface <name1>, <name2>, ...
config redistribute
    Description: Redistribute configuration.
    edit <name>
        set status [enable|disable]
        set metric {integer}
        set routemap {string}
        set metric-type [1|2]
        set tag {integer}
    next
end
set restart-mode [none|lls|...]
set restart-period {integer}
set rfc1583-compatible [enable|disable]
set router-id {ipv4-address-any}
set spf-timers {user}
config summary-address
    Description: IP address summary configuration.
    edit <id>
        set prefix {ipv4-classnet}
        set tag {integer}

```

```

        set advertise [disable|enable]
    next
end
end

```

## config router ospf

Parameter	Description	Type	Size	Default										
abr-type	Area border router type.	option	-	standard										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>cisco</td><td>Cisco.</td></tr><tr><td>ibm</td><td>IBM.</td></tr><tr><td>shortcut</td><td>Shortcut.</td></tr><tr><td>standard</td><td>Standard.</td></tr></table>	Option	Description	cisco	Cisco.	ibm	IBM.	shortcut	Shortcut.	standard	Standard.			
	Option	Description												
	cisco	Cisco.												
	ibm	IBM.												
	shortcut	Shortcut.												
standard	Standard.													
auto-cost-ref-bandwidth	Reference bandwidth in terms of megabits per second.	integer	Minimum value: 1 Maximum value: 1000000	1000										
bfd	Bidirectional Forwarding Detection (BFD).	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>	Option	Description	enable	Enable setting.	disable	Disable setting.							
	Option	Description												
	enable	Enable setting.												
disable	Disable setting.													
database-overflow	Enable/disable database overflow.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>	Option	Description	enable	Enable setting.	disable	Disable setting.							
	Option	Description												
	enable	Enable setting.												
disable	Disable setting.													
database-overflow-max-lsas	Database overflow maximum LSAs.	integer	Minimum value: 0 Maximum value: 4294967295	10000										
database-overflow-time-to-recover	Database overflow time to recover (sec).	integer	Minimum value: 0 Maximum value: 65535	300										

Parameter	Description	Type	Size	Default								
default-information-metric	Default information metric.	integer	Minimum value: 1 Maximum value: 16777214	10								
default-information-metric-type	Default information metric type.	option	-	2								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>1</td><td>Type 1.</td></tr><tr><td>2</td><td>Type 2.</td></tr></table>				Option	Description	1	Type 1.	2	Type 2.		
Option	Description											
1	Type 1.											
2	Type 2.											
default-information-originate	Enable/disable generation of default route.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>always</i></td><td>Always advertise the default router.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>				Option	Description	<i>enable</i>	Enable setting.	<i>always</i>	Always advertise the default router.	<i>disable</i>	Disable setting.
Option	Description											
<i>enable</i>	Enable setting.											
<i>always</i>	Always advertise the default router.											
<i>disable</i>	Disable setting.											
default-information-route-map	Default information route map.	string	Maximum length: 35									
default-metric	Default metric of redistribute routes.	integer	Minimum value: 1 Maximum value: 16777214	10								
distance	Distance of the route.	integer	Minimum value: 1 Maximum value: 255	110								
distance-external	Administrative external distance.	integer	Minimum value: 1 Maximum value: 255	110								

Parameter	Description	Type	Size	Default								
distance-inter-area	Administrative inter-area distance.	integer	Minimum value: 1 Maximum value: 255	110								
distance-intra-area	Administrative intra-area distance.	integer	Minimum value: 1 Maximum value: 255	110								
distribute-list-in	Filter incoming routes.	string	Maximum length: 35									
distribute-route-map-in	Filter incoming external routes by route-map.	string	Maximum length: 35									
log-neighbour-changes	Log of OSPF neighbor changes.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
passive-interface <name>	Passive interface configuration. Passive interface name.	string	Maximum length: 79									
restart-mode	OSPF restart mode (graceful or LLS).	option	-	none								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>Hitless restart disabled.</td></tr><tr><td><i>lls</i></td><td>LLS mode.</td></tr><tr><td><i>graceful-restart</i></td><td>Graceful Restart Mode.</td></tr></table>	Option	Description	<i>none</i>	Hitless restart disabled.	<i>lls</i>	LLS mode.	<i>graceful-restart</i>	Graceful Restart Mode.			
Option	Description											
<i>none</i>	Hitless restart disabled.											
<i>lls</i>	LLS mode.											
<i>graceful-restart</i>	Graceful Restart Mode.											
restart-period	Graceful restart period.	integer	Minimum value: 1 Maximum value: 3600	120								
rfc1583-compatible	Enable/disable RFC1583 compatibility.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											

Parameter	Description	Type	Size	Default
router-id	Router ID.	ipv4-address-any	Not Specified	0.0.0.0
spf-timers	SPF calculation frequency.	user	Not Specified	

## config area

Parameter	Description	Type	Size	Default								
id	Area entry IP address.	ipv4-address-any	Not Specified	0.0.0.0								
shortcut	Enable/disable shortcut option.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable shortcut option.</td></tr><tr><td><i>enable</i></td><td>Enable shortcut option.</td></tr><tr><td><i>default</i></td><td>Default shortcut option.</td></tr></table>	Option	Description	<i>disable</i>	Disable shortcut option.	<i>enable</i>	Enable shortcut option.	<i>default</i>	Default shortcut option.			
	Option	Description										
	<i>disable</i>	Disable shortcut option.										
	<i>enable</i>	Enable shortcut option.										
<i>default</i>	Default shortcut option.											
authentication	Authentication type.	option	-	none								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>None.</td></tr><tr><td><i>text</i></td><td>Text.</td></tr><tr><td><i>message-digest</i></td><td>Message digest.</td></tr></table>	Option	Description	<i>none</i>	None.	<i>text</i>	Text.	<i>message-digest</i>	Message digest.			
	Option	Description										
	<i>none</i>	None.										
	<i>text</i>	Text.										
<i>message-digest</i>	Message digest.											
default-cost	Summary default cost of stub or NSSA area.	integer	Minimum value: 0 Maximum value: 4294967295	10								
nssa-translator-role	NSSA translator role type.	option	-	candidate								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>candidate</i></td><td>Candidate.</td></tr><tr><td><i>never</i></td><td>Never.</td></tr><tr><td><i>always</i></td><td>Always.</td></tr></table>	Option	Description	<i>candidate</i>	Candidate.	<i>never</i>	Never.	<i>always</i>	Always.			
	Option	Description										
	<i>candidate</i>	Candidate.										
	<i>never</i>	Never.										
<i>always</i>	Always.											
stub-type	Stub summary setting.	option	-	summary								



Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>no-summary</i></td><td>No summary.</td></tr><tr><td><i>summary</i></td><td>Summary.</td></tr></table>	Option	Description	<i>no-summary</i>	No summary.	<i>summary</i>	Summary.					
	Option	Description										
	<i>no-summary</i>	No summary.										
<i>summary</i>	Summary.											
type	Area type setting.	option	-	regular								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>regular</i></td><td>Regular.</td></tr><tr><td><i>nssa</i></td><td>NSSA.</td></tr><tr><td><i>stub</i></td><td>Stub.</td></tr></table>	Option	Description	<i>regular</i>	Regular.	<i>nssa</i>	NSSA.	<i>stub</i>	Stub.			
	Option	Description										
	<i>regular</i>	Regular.										
	<i>nssa</i>	NSSA.										
<i>stub</i>	Stub.											
nssa-default-information-originate	Redistribute, advertise, or do not originate Type-7 default route into NSSA area.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Redistribute Type-7 default route from routing table.</td></tr><tr><td><i>always</i></td><td>Advertise a self-originated Type-7 default route.</td></tr><tr><td><i>disable</i></td><td>Do not advertise Type-7 default route.</td></tr></table>	Option	Description	<i>enable</i>	Redistribute Type-7 default route from routing table.	<i>always</i>	Advertise a self-originated Type-7 default route.	<i>disable</i>	Do not advertise Type-7 default route.			
	Option	Description										
	<i>enable</i>	Redistribute Type-7 default route from routing table.										
	<i>always</i>	Advertise a self-originated Type-7 default route.										
<i>disable</i>	Do not advertise Type-7 default route.											
nssa-default-information-originate-metric	OSPF default metric.	integer	Minimum value: 0 Maximum value: 16777214	10								
nssa-default-information-originate-metric-type	OSPF metric type for default routes.	option	-	2								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>1</td><td>Type 1.</td></tr><tr><td>2</td><td>Type 2.</td></tr></table>	Option	Description	1	Type 1.	2	Type 2.					
	Option	Description										
	1	Type 1.										
2	Type 2.											
nssa-redistribution	Enable/disable redistribute into NSSA area.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable redistribute into NSSA area.</td></tr><tr><td><i>disable</i></td><td>Disable redistribute into NSSA area.</td></tr></table>	Option	Description	<i>enable</i>	Enable redistribute into NSSA area.	<i>disable</i>	Disable redistribute into NSSA area.					
	Option	Description										
	<i>enable</i>	Enable redistribute into NSSA area.										
<i>disable</i>	Disable redistribute into NSSA area.											

Parameter	Description	Type	Size	Default
comments	Comment.	var-string	Maximum length: 255	

#### config range

Parameter	Description	Type	Size	Default						
id	Range entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0						
prefix	Prefix.	ipv4-classnet-any	Not Specified	0.0.0.0 0.0.0.0						
advertise	Enable/disable advertise status.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable advertise status.</td></tr><tr><td><i>enable</i></td><td>Enable advertise status.</td></tr></table>				Option	Description	<i>disable</i>	Disable advertise status.	<i>enable</i>	Enable advertise status.
Option	Description									
<i>disable</i>	Disable advertise status.									
<i>enable</i>	Enable advertise status.									
substitute	Substitute prefix.	ipv4-classnet-any	Not Specified	0.0.0.0 0.0.0.0						
substitute-status	Enable/disable substitute status.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable substitute status.</td></tr><tr><td><i>disable</i></td><td>Disable substitute status.</td></tr></table>				Option	Description	<i>enable</i>	Enable substitute status.	<i>disable</i>	Disable substitute status.
Option	Description									
<i>enable</i>	Enable substitute status.									
<i>disable</i>	Disable substitute status.									

#### config virtual-link

Parameter	Description	Type	Size	Default				
name	Virtual link entry name.	string	Maximum length: 35					
authentication	Authentication type.	option	-	none				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>None.</td></tr></table>				Option	Description	<i>none</i>	None.
Option	Description							
<i>none</i>	None.							

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>text</i>	Text.		
	<i>message-digest</i>	Message digest.		
authentication-key	Authentication key.	password	Not Specified	
keychain	Message-digest key-chain name.	string	Maximum length: 35	
dead-interval	Dead interval.	integer	Minimum value: 1 Maximum value: 65535	40
hello-interval	Hello interval.	integer	Minimum value: 1 Maximum value: 65535	10
retransmit-interval	Retransmit interval.	integer	Minimum value: 1 Maximum value: 65535	5
transmit-delay	Transmit delay.	integer	Minimum value: 1 Maximum value: 65535	1
peer	Peer IP.	ipv4-address-any	Not Specified	0.0.0.0

### config md5-keys

Parameter	Description	Type	Size	Default
id	Key ID.	integer	Minimum value: 1 Maximum value: 255	0
key-string	Password for the key.	password	Not Specified	

### config md5-keys

Parameter	Description	Type	Size	Default
id	Key ID.	integer	Minimum value: 1 Maximum value: 255	0
key-string	Password for the key.	password	Not Specified	

### config filter-list

Parameter	Description	Type	Size	Default						
id	Filter list entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0						
list	Access-list or prefix-list name.	string	Maximum length: 35							
direction	Direction.	option	-	out						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>in</i></td><td>In.</td></tr><tr><td><i>out</i></td><td>Out.</td></tr></table>				Option	Description	<i>in</i>	In.	<i>out</i>	Out.
Option	Description									
<i>in</i>	In.									
<i>out</i>	Out.									

### config distribute-list

Parameter	Description	Type	Size	Default				
id	Distribute list entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0				
access-list	Access list name.	string	Maximum length: 35					
protocol	Protocol type.	option	-	connected				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>connected</i></td><td>Connected type.</td></tr></table>	Option	Description	<i>connected</i>	Connected type.			
Option	Description							
<i>connected</i>	Connected type.							

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>static</i>	Static type.		
	<i>rip</i>	RIP type.		

### config neighbor

Parameter	Description	Type	Size	Default
id	Neighbor entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
ip	Interface IP address of the neighbor.	ipv4-address	Not Specified	0.0.0.0
poll-interval	Poll interval time in seconds.	integer	Minimum value: 1 Maximum value: 65535	10
cost	Cost of the interface, value range from 0 to 65535, 0 means auto-cost.	integer	Minimum value: 0 Maximum value: 65535	0
priority	Priority.	integer	Minimum value: 0 Maximum value: 255	1

### config network

Parameter	Description	Type	Size	Default
id	Network entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
prefix	Prefix.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0

Parameter	Description	Type	Size	Default
area	Attach the network to area.	ipv4-address-any	Not Specified	0.0.0.0
comments	Comment.	var-string	Maximum length: 255	

## config ospf-interface

Parameter	Description	Type	Size	Default								
name	Interface entry name.	string	Maximum length: 35									
comments	Comment.	var-string	Maximum length: 255									
interface	Configuration interface name.	string	Maximum length: 15									
ip	IP address.	ipv4-address	Not Specified	0.0.0.0								
authentication	Authentication type.	option	-	none								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>None.</td></tr><tr><td><i>text</i></td><td>Text.</td></tr><tr><td><i>message-digest</i></td><td>Message digest.</td></tr></table>				Option	Description	<i>none</i>	None.	<i>text</i>	Text.	<i>message-digest</i>	Message digest.
Option	Description											
<i>none</i>	None.											
<i>text</i>	Text.											
<i>message-digest</i>	Message digest.											
authentication-key	Authentication key.	password	Not Specified									
keychain	Message-digest key-chain name.	string	Maximum length: 35									
prefix-length	Prefix length.	integer	Minimum value: 0 Maximum value: 32	0								
retransmit-interval	Retransmit interval.	integer	Minimum value: 1 Maximum value: 65535	5								

Parameter	Description	Type	Size	Default						
transmit-delay	Transmit delay.	integer	Minimum value: 1 Maximum value: 65535	1						
cost	Cost of the interface, value range from 0 to 65535, 0 means auto-cost.	integer	Minimum value: 0 Maximum value: 65535	0						
priority	Priority.	integer	Minimum value: 0 Maximum value: 255	1						
dead-interval	Dead interval.	integer	Minimum value: 0 Maximum value: 65535	0						
hello-interval	Hello interval.	integer	Minimum value: 0 Maximum value: 65535	0						
hello-multiplier	Number of hello packets within dead interval.	integer	Minimum value: 3 Maximum value: 10	0						
database-filter-out	Enable/disable control of flooding out LSAs.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>				Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
mtu	MTU for database description packets.	integer	Minimum value: 576 Maximum value: 65535	0						
mtu-ignore	Enable/disable ignore MTU.	option	-	disable						

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
network-type	Network type.	option	-	broadcast
	<b>Option</b>	<b>Description</b>		
	<i>broadcast</i>	Broadcast.		
	<i>non-broadcast</i>	Non-broadcast.		
	<i>point-to-point</i>	Point-to-point.		
	<i>point-to-multipoint</i>	Point-to-multipoint.		
	<i>point-to-multipoint-non-broadcast</i>	Point-to-multipoint and non-broadcast.		
bfd	Bidirectional Forwarding Detection (BFD).	option	-	global
	<b>Option</b>	<b>Description</b>		
	<i>global</i>	Follow global configuration.		
	<i>enable</i>	Enable BFD on this interface.		
	<i>disable</i>	Disable BFD on this interface.		
status	Enable/disable status.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
resync-timeout	Graceful restart neighbor resynchronization timeout.	integer	Minimum value: 1 Maximum value: 3600	40



## config md5-keys

Parameter	Description	Type	Size	Default
id	Key ID.	integer	Minimum value: 1 Maximum value: 255	0
key-string	Password for the key.	password	Not Specified	

## config md5-keys

Parameter	Description	Type	Size	Default
id	Key ID.	integer	Minimum value: 1 Maximum value: 255	0
key-string	Password for the key.	password	Not Specified	

## config redistribute

Parameter	Description	Type	Size	Default
name	Redistribute name.	string	Maximum length: 35	
status	Status.	option	-	disable
	Option	Description		
	enable	Enable setting.		
	disable	Disable setting.		
metric	Redistribute metric setting.	integer	Minimum value: 0 Maximum value: 16777214	0
routemap	Route map name.	string	Maximum length: 35	
metric-type	Metric type.	option	-	2

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	1	Type 1.		
	2	Type 2.		
tag	Tag value.	integer	Minimum value: 0 Maximum value: 4294967295	0

### config summary-address

Parameter	Description	Type	Size	Default
id	Summary address entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
prefix	Prefix.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0
tag	Tag value.	integer	Minimum value: 0 Maximum value: 4294967295	0
advertise	Enable/disable advertise status.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable advertise status.		
	<i>enable</i>	Enable advertise status.		

## config router ospf6

Configure IPv6 OSPF.

```
config router ospf6
  Description: Configure IPv6 OSPF.
  set abr-type [cisco|ibm|...]
  config area
    Description: OSPF6 area configuration.
    edit <id>
      set default-cost {integer}
      set nssa-translator-role [candidate|never|...]
```

```

set stub-type [no-summary|summary]
set type [regular|nssa|...]
set nssa-default-information-originate [enable|disable]
set nssa-default-information-originate-metric {integer}
set nssa-default-information-originate-metric-type [1|2]
set nssa-redistribution [enable|disable]
set authentication [none|ah|...]
set key-rollover-interval {integer}
set ipsec-auth-alg [md5|sha1|...]
set ipsec-enc-alg [null|des|...]
config ipsec-keys
    Description: IPsec authentication and encryption keys.
    edit <spi>
        set auth-key {password}
        set enc-key {password}
    next
end
config range
    Description: OSPF6 area range configuration.
    edit <id>
        set prefix6 {ipv6-network}
        set advertise [disable|enable]
    next
end
config virtual-link
    Description: OSPF6 virtual link configuration.
    edit <name>
        set dead-interval {integer}
        set hello-interval {integer}
        set retransmit-interval {integer}
        set transmit-delay {integer}
        set peer {ipv4-address-any}
        set authentication [none|ah|...]
        set key-rollover-interval {integer}
        set ipsec-auth-alg [md5|sha1|...]
        set ipsec-enc-alg [null|des|...]
        config ipsec-keys
            Description: IPsec authentication and encryption keys.
            edit <spi>
                set auth-key {password}
                set enc-key {password}
            next
        end
    next
end
next
end
set auto-cost-ref-bandwidth {integer}
set bfd [enable|disable]
set default-information-metric {integer}
set default-information-metric-type [1|2]
set default-information-originate [enable|always|...]
set default-information-route-map {string}
set default-metric {integer}
set log-neighbour-changes [enable|disable]
config ospf6-interface

```

```

Description: OSPF6 interface configuration.
edit <name>
    set area-id {ipv4-address-any}
    set interface {string}
    set retransmit-interval {integer}
    set transmit-delay {integer}
    set cost {integer}
    set priority {integer}
    set dead-interval {integer}
    set hello-interval {integer}
    set status [disable|enable]
    set network-type [broadcast|point-to-point|...]
    set bfd [global|enable|...]
    set mtu {integer}
    set mtu-ignore [enable|disable]
    set authentication [none|ah|...]
    set key-rollover-interval {integer}
    set ipsec-auth-alg [md5|sha1|...]
    set ipsec-enc-alg [null|des|...]
    config ipsec-keys
        Description: IPsec authentication and encryption keys.
        edit <spi>
            set auth-key {password}
            set enc-key {password}
        next
    end
    config neighbor
        Description: OSPFv3 neighbors are used when OSPFv3 runs on non-broadcast
media.
        edit <ip6>
            set poll-interval {integer}
            set cost {integer}
            set priority {integer}
        next
    end
next
end
set passive-interface <name1>, <name2>, ...
config redistribute
    Description: Redistribute configuration.
    edit <name>
        set status [enable|disable]
        set metric {integer}
        set routemap {string}
        set metric-type [1|2]
    next
end
set router-id {ipv4-address-any}
set spf-timers {user}
config summary-address
    Description: IPv6 address summary configuration.
    edit <id>
        set prefix6 {ipv6-network}
        set advertise [disable|enable]
        set tag {integer}
    next

```

end  
end

## config router ospf6

Parameter	Description	Type	Size	Default								
abr-type	Area border router type.	option	-	standard								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>cisco</td><td>Cisco.</td></tr><tr><td>ibm</td><td>IBM.</td></tr><tr><td>standard</td><td>Standard.</td></tr></table>	Option	Description	cisco	Cisco.	ibm	IBM.	standard	Standard.			
	Option	Description										
	cisco	Cisco.										
	ibm	IBM.										
standard	Standard.											
auto-cost-ref-bandwidth	Reference bandwidth in terms of megabits per second.	integer	Minimum value: 1 Maximum value: 1000000	1000								
bfd	Enable/disable Bidirectional Forwarding Detection (BFD).	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable Bidirectional Forwarding Detection (BFD).</td></tr><tr><td>disable</td><td>Disable Bidirectional Forwarding Detection (BFD).</td></tr></table>	Option	Description	enable	Enable Bidirectional Forwarding Detection (BFD).	disable	Disable Bidirectional Forwarding Detection (BFD).					
	Option	Description										
	enable	Enable Bidirectional Forwarding Detection (BFD).										
disable	Disable Bidirectional Forwarding Detection (BFD).											
default-information-metric	Default information metric.	integer	Minimum value: 1 Maximum value: 16777214	10								
default-information-metric-type	Default information metric type.	option	-	2								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>1</td><td>Type 1.</td></tr><tr><td>2</td><td>Type 2.</td></tr></table>	Option	Description	1	Type 1.	2	Type 2.					
	Option	Description										
	1	Type 1.										
2	Type 2.											
default-information-originate	Enable/disable generation of default route.	option	-	disable								

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>always</i>	Always advertise the default router.		
	<i>disable</i>	Disable setting.		
default-information-route-map	Default information route map.	string	Maximum length: 35	
default-metric	Default metric of redistribute routes.	integer	Minimum value: 1 Maximum value: 16777214	10
log-neighbour-changes	Log OSPFv3 neighbor changes.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
passive-interface <name>	Passive interface configuration. Passive interface name.	string	Maximum length: 79	
router-id	A.B.C.D, in IPv4 address format.	ipv4-address-any	Not Specified	0.0.0.0
spf-timers	SPF calculation frequency.	user	Not Specified	

## config area

Parameter	Description	Type	Size	Default
id	Area entry IP address.	ipv4-address-any	Not Specified	0.0.0.0

Parameter	Description	Type	Size	Default								
default-cost	Summary default cost of stub or NSSA area.	integer	Minimum value: 0 Maximum value: 16777215	10								
nssa-translator-role	NSSA translator role type.	option	-	candidate								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>candidate</i></td><td>Candidate.</td></tr><tr><td><i>never</i></td><td>Never.</td></tr><tr><td><i>always</i></td><td>Always.</td></tr></table>	Option	Description	<i>candidate</i>	Candidate.	<i>never</i>	Never.	<i>always</i>	Always.			
Option	Description											
<i>candidate</i>	Candidate.											
<i>never</i>	Never.											
<i>always</i>	Always.											
stub-type	Stub summary setting.	option	-	summary								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>no-summary</i></td><td>No summary.</td></tr><tr><td><i>summary</i></td><td>Summary.</td></tr></table>	Option	Description	<i>no-summary</i>	No summary.	<i>summary</i>	Summary.					
Option	Description											
<i>no-summary</i>	No summary.											
<i>summary</i>	Summary.											
type	Area type setting.	option	-	regular								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>regular</i></td><td>Regular.</td></tr><tr><td><i>nssa</i></td><td>NSSA.</td></tr><tr><td><i>stub</i></td><td>Stub.</td></tr></table>	Option	Description	<i>regular</i>	Regular.	<i>nssa</i>	NSSA.	<i>stub</i>	Stub.			
Option	Description											
<i>regular</i>	Regular.											
<i>nssa</i>	NSSA.											
<i>stub</i>	Stub.											
nssa-default-information-originate	Enable/disable originate type 7 default into NSSA area.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable originate type 7 default into NSSA area.</td></tr><tr><td><i>disable</i></td><td>Disable originate type 7 default into NSSA area.</td></tr></table>	Option	Description	<i>enable</i>	Enable originate type 7 default into NSSA area.	<i>disable</i>	Disable originate type 7 default into NSSA area.					
Option	Description											
<i>enable</i>	Enable originate type 7 default into NSSA area.											
<i>disable</i>	Disable originate type 7 default into NSSA area.											
nssa-default-information-originate-metric	OSPFv3 default metric.	integer	Minimum value: 0 Maximum value: 16777214	10								

Parameter	Description	Type	Size	Default												
nssa-default-information-originate-metric-type	OSPFv3 metric type for default routes.	option	-	2												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>1</td><td>Type 1.</td></tr><tr><td>2</td><td>Type 2.</td></tr></table>	Option	Description	1	Type 1.	2	Type 2.									
	Option	Description														
	1	Type 1.														
2	Type 2.															
nssa-redistribution	Enable/disable redistribute into NSSA area.	option	-	enable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable redistribute into NSSA area.</td></tr><tr><td>disable</td><td>Disable redistribute into NSSA area.</td></tr></table>	Option	Description	enable	Enable redistribute into NSSA area.	disable	Disable redistribute into NSSA area.									
	Option	Description														
	enable	Enable redistribute into NSSA area.														
disable	Disable redistribute into NSSA area.															
authentication	Authentication mode.	option	-	none												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>none</td><td>Disable authentication.</td></tr><tr><td>ah</td><td>Authentication Header.</td></tr><tr><td>esp</td><td>Encapsulating Security Payload.</td></tr></table>	Option	Description	none	Disable authentication.	ah	Authentication Header.	esp	Encapsulating Security Payload.							
	Option	Description														
	none	Disable authentication.														
	ah	Authentication Header.														
esp	Encapsulating Security Payload.															
key-rollover-interval	Key roll-over interval.	integer	Minimum value: 300 Maximum value: 216000	300												
ipsec-auth-alg	Authentication algorithm.	option	-	md5												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>md5</td><td>MD5.</td></tr><tr><td>sha1</td><td>SHA1.</td></tr><tr><td>sha256</td><td>SHA256.</td></tr><tr><td>sha384</td><td>SHA384.</td></tr><tr><td>sha512</td><td>SHA512.</td></tr></table>	Option	Description	md5	MD5.	sha1	SHA1.	sha256	SHA256.	sha384	SHA384.	sha512	SHA512.			
	Option	Description														
	md5	MD5.														
	sha1	SHA1.														
	sha256	SHA256.														
	sha384	SHA384.														
sha512	SHA512.															
ipsec-enc-alg	Encryption algorithm.	option	-	null												



Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>null</i>	No encryption.		
	<i>des</i>	DES.		
	<i>3des</i>	3DES.		
	<i>aes128</i>	AES128.		
	<i>aes192</i>	AES192.		
	<i>aes256</i>	AES256.		

#### config ipsec-keys

Parameter	Description	Type	Size	Default
spi	Security Parameters Index.	integer	Minimum value: 256 Maximum value: 4294967295	0
auth-key	Authentication key.	password	Not Specified	
enc-key	Encryption key.	password	Not Specified	

#### config ipsec-keys

Parameter	Description	Type	Size	Default
spi	Security Parameters Index.	integer	Minimum value: 256 Maximum value: 4294967295	0
auth-key	Authentication key.	password	Not Specified	
enc-key	Encryption key.	password	Not Specified	

## config range

Parameter	Description	Type	Size	Default						
id	Range entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0						
prefix6	IPv6 prefix.	ipv6-network	Not Specified	::/0						
advertise	Enable/disable advertise status.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>disable</td></tr><tr><td><i>enable</i></td><td>enable</td></tr></table>				Option	Description	<i>disable</i>	disable	<i>enable</i>	enable
	Option	Description								
	<i>disable</i>	disable								
<i>enable</i>	enable									

## config virtual-link

Parameter	Description	Type	Size	Default
name	Virtual link entry name.	string	Maximum length: 35	
dead-interval	Dead interval.	integer	Minimum value: 1 Maximum value: 65535	40
hello-interval	Hello interval.	integer	Minimum value: 1 Maximum value: 65535	10
retransmit-interval	Retransmit interval.	integer	Minimum value: 1 Maximum value: 65535	5
transmit-delay	Transmit delay.	integer	Minimum value: 1 Maximum value: 65535	1

Parameter	Description	Type	Size	Default														
peer	A.B.C.D, peer router ID.	ipv4-address-any	Not Specified	0.0.0.0														
authentication	Authentication mode.	option	-	area														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>Disable authentication.</td></tr><tr><td><i>ah</i></td><td>Authentication Header.</td></tr><tr><td><i>esp</i></td><td>Encapsulating Security Payload.</td></tr><tr><td><i>area</i></td><td>Use the routing area's authentication configuration.</td></tr></table>	Option	Description	<i>none</i>	Disable authentication.	<i>ah</i>	Authentication Header.	<i>esp</i>	Encapsulating Security Payload.	<i>area</i>	Use the routing area's authentication configuration.							
	Option	Description																
	<i>none</i>	Disable authentication.																
	<i>ah</i>	Authentication Header.																
	<i>esp</i>	Encapsulating Security Payload.																
	<i>area</i>	Use the routing area's authentication configuration.																
key-rollover-interval	Key roll-over interval.	integer	Minimum value: 300 Maximum value: 216000	300														
ipsec-auth-alg	Authentication algorithm.	option	-	md5														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>md5</i></td><td>MD5.</td></tr><tr><td><i>sha1</i></td><td>SHA1.</td></tr><tr><td><i>sha256</i></td><td>SHA256.</td></tr><tr><td><i>sha384</i></td><td>SHA384.</td></tr><tr><td><i>sha512</i></td><td>SHA512.</td></tr></table>	Option	Description	<i>md5</i>	MD5.	<i>sha1</i>	SHA1.	<i>sha256</i>	SHA256.	<i>sha384</i>	SHA384.	<i>sha512</i>	SHA512.					
	Option	Description																
	<i>md5</i>	MD5.																
	<i>sha1</i>	SHA1.																
	<i>sha256</i>	SHA256.																
	<i>sha384</i>	SHA384.																
	<i>sha512</i>	SHA512.																
ipsec-enc-alg	Encryption algorithm.	option	-	null														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>null</i></td><td>No encryption.</td></tr><tr><td><i>des</i></td><td>DES.</td></tr><tr><td><i>3des</i></td><td>3DES.</td></tr><tr><td><i>aes128</i></td><td>AES128.</td></tr><tr><td><i>aes192</i></td><td>AES192.</td></tr><tr><td><i>aes256</i></td><td>AES256.</td></tr></table>	Option	Description	<i>null</i>	No encryption.	<i>des</i>	DES.	<i>3des</i>	3DES.	<i>aes128</i>	AES128.	<i>aes192</i>	AES192.	<i>aes256</i>	AES256.			
	Option	Description																
	<i>null</i>	No encryption.																
	<i>des</i>	DES.																
	<i>3des</i>	3DES.																
	<i>aes128</i>	AES128.																
	<i>aes192</i>	AES192.																
	<i>aes256</i>	AES256.																

### config ipsec-keys

Parameter	Description	Type	Size	Default
spi	Security Parameters Index.	integer	Minimum value: 256 Maximum value: 4294967295	0
auth-key	Authentication key.	password	Not Specified	
enc-key	Encryption key.	password	Not Specified	

### config ipsec-keys

Parameter	Description	Type	Size	Default
spi	Security Parameters Index.	integer	Minimum value: 256 Maximum value: 4294967295	0
auth-key	Authentication key.	password	Not Specified	
enc-key	Encryption key.	password	Not Specified	

### config ospf6-interface

Parameter	Description	Type	Size	Default
name	Interface entry name.	string	Maximum length: 35	
area-id	A.B.C.D, in IPv4 address format.	ipv4-address-any	Not Specified	0.0.0.0
interface	Configuration interface name.	string	Maximum length: 15	
retransmit-interval	Retransmit interval.	integer	Minimum value: 1 Maximum value: 65535	5

Parameter	Description	Type	Size	Default										
transmit-delay	Transmit delay.	integer	Minimum value: 1 Maximum value: 65535	1										
cost	Cost of the interface, value range from 0 to 65535, 0 means auto-cost.	integer	Minimum value: 0 Maximum value: 65535	0										
priority	Priority.	integer	Minimum value: 0 Maximum value: 255	1										
dead-interval	Dead interval.	integer	Minimum value: 1 Maximum value: 65535	0										
hello-interval	Hello interval.	integer	Minimum value: 1 Maximum value: 65535	0										
status	Enable/disable OSPF6 routing on this interface.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable OSPF6 routing.</td></tr><tr><td><i>enable</i></td><td>Enable OSPF6 routing.</td></tr></table>	Option	Description	<i>disable</i>	Disable OSPF6 routing.	<i>enable</i>	Enable OSPF6 routing.							
Option	Description													
<i>disable</i>	Disable OSPF6 routing.													
<i>enable</i>	Enable OSPF6 routing.													
network-type	Network type.	option	-	broadcast										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>broadcast</i></td><td>broadcast</td></tr><tr><td><i>point-to-point</i></td><td>point-to-point</td></tr><tr><td><i>non-broadcast</i></td><td>non-broadcast</td></tr><tr><td><i>point-to-multipoint</i></td><td>point-to-multipoint</td></tr></table>	Option	Description	<i>broadcast</i>	broadcast	<i>point-to-point</i>	point-to-point	<i>non-broadcast</i>	non-broadcast	<i>point-to-multipoint</i>	point-to-multipoint			
Option	Description													
<i>broadcast</i>	broadcast													
<i>point-to-point</i>	point-to-point													
<i>non-broadcast</i>	non-broadcast													
<i>point-to-multipoint</i>	point-to-multipoint													

Parameter	Description	Type	Size	Default										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>point-to-multipoint-non-broadcast</i></td><td>point-to-multipoint and non-broadcast.</td></tr></table>	Option	Description	<i>point-to-multipoint-non-broadcast</i>	point-to-multipoint and non-broadcast.									
Option	Description													
<i>point-to-multipoint-non-broadcast</i>	point-to-multipoint and non-broadcast.													
bfd	Enable/disable Bidirectional Forwarding Detection (BFD).	option	-	global										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>global</i></td><td>Use global configuration of Bidirectional Forwarding Detection (BFD).</td></tr><tr><td><i>enable</i></td><td>Enable Bidirectional Forwarding Detection (BFD) on this interface.</td></tr><tr><td><i>disable</i></td><td>Disable Bidirectional Forwarding Detection (BFD) on this interface.</td></tr></table>	Option	Description	<i>global</i>	Use global configuration of Bidirectional Forwarding Detection (BFD).	<i>enable</i>	Enable Bidirectional Forwarding Detection (BFD) on this interface.	<i>disable</i>	Disable Bidirectional Forwarding Detection (BFD) on this interface.					
Option	Description													
<i>global</i>	Use global configuration of Bidirectional Forwarding Detection (BFD).													
<i>enable</i>	Enable Bidirectional Forwarding Detection (BFD) on this interface.													
<i>disable</i>	Disable Bidirectional Forwarding Detection (BFD) on this interface.													
mtu	MTU for OSPFv3 packets.	integer	Minimum value: 576 Maximum value: 65535	0										
mtu-ignore	Enable/disable ignoring MTU field in DBD packets.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Ignore MTU field in DBD packets.</td></tr><tr><td><i>disable</i></td><td>Do not ignore MTU field in DBD packets.</td></tr></table>	Option	Description	<i>enable</i>	Ignore MTU field in DBD packets.	<i>disable</i>	Do not ignore MTU field in DBD packets.							
Option	Description													
<i>enable</i>	Ignore MTU field in DBD packets.													
<i>disable</i>	Do not ignore MTU field in DBD packets.													
authentication	Authentication mode.	option	-	area										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>Disable authentication.</td></tr><tr><td><i>ah</i></td><td>Authentication Header.</td></tr><tr><td><i>esp</i></td><td>Encapsulating Security Payload.</td></tr><tr><td><i>area</i></td><td>Use the routing area's authentication configuration.</td></tr></table>	Option	Description	<i>none</i>	Disable authentication.	<i>ah</i>	Authentication Header.	<i>esp</i>	Encapsulating Security Payload.	<i>area</i>	Use the routing area's authentication configuration.			
Option	Description													
<i>none</i>	Disable authentication.													
<i>ah</i>	Authentication Header.													
<i>esp</i>	Encapsulating Security Payload.													
<i>area</i>	Use the routing area's authentication configuration.													
key-rollover-interval	Key roll-over interval.	integer	Minimum value: 300 Maximum value: 216000	300										
ipsec-auth-alg	Authentication algorithm.	option	-	md5										

Parameter	Description	Type	Size	Default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>md5</i></td><td>MD5.</td></tr><tr><td><i>sha1</i></td><td>SHA1.</td></tr><tr><td><i>sha256</i></td><td>SHA256.</td></tr><tr><td><i>sha384</i></td><td>SHA384.</td></tr><tr><td><i>sha512</i></td><td>SHA512.</td></tr></table>	Option	Description	<i>md5</i>	MD5.	<i>sha1</i>	SHA1.	<i>sha256</i>	SHA256.	<i>sha384</i>	SHA384.	<i>sha512</i>	SHA512.					
	Option	Description																
	<i>md5</i>	MD5.																
	<i>sha1</i>	SHA1.																
	<i>sha256</i>	SHA256.																
	<i>sha384</i>	SHA384.																
	<i>sha512</i>	SHA512.																
ipsec-enc-alg	Encryption algorithm.	option	-	null														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>null</i></td><td>No encryption.</td></tr><tr><td><i>des</i></td><td>DES.</td></tr><tr><td><i>3des</i></td><td>3DES.</td></tr><tr><td><i>aes128</i></td><td>AES128.</td></tr><tr><td><i>aes192</i></td><td>AES192.</td></tr><tr><td><i>aes256</i></td><td>AES256.</td></tr></table>	Option	Description	<i>null</i>	No encryption.	<i>des</i>	DES.	<i>3des</i>	3DES.	<i>aes128</i>	AES128.	<i>aes192</i>	AES192.	<i>aes256</i>	AES256.			
	Option	Description																
	<i>null</i>	No encryption.																
	<i>des</i>	DES.																
	<i>3des</i>	3DES.																
	<i>aes128</i>	AES128.																
	<i>aes192</i>	AES192.																
<i>aes256</i>	AES256.																	

#### config ipsec-keys

Parameter	Description	Type	Size	Default
spi	Security Parameters Index.	integer	Minimum value: 256 Maximum value: 4294967295	0
auth-key	Authentication key.	password	Not Specified	
enc-key	Encryption key.	password	Not Specified	

#### config ipsec-keys

Parameter	Description	Type	Size	Default
spi	Security Parameters Index.	integer	Minimum value: 256 Maximum value: 4294967295	0
auth-key	Authentication key.	password	Not Specified	

Parameter	Description	Type	Size	Default
enc-key	Encryption key.	password	Not Specified	

### config neighbor

Parameter	Description	Type	Size	Default
ip6	IPv6 link local address of the neighbor.	ipv6-address	Not Specified	::
poll-interval	Poll interval time in seconds.	integer	Minimum value: 1 Maximum value: 65535	10
cost	Cost of the interface, value range from 0 to 65535, 0 means auto-cost.	integer	Minimum value: 0 Maximum value: 65535	0
priority	Priority.	integer	Minimum value: 0 Maximum value: 255	1

### config redistribute

Parameter	Description	Type	Size	Default						
name	Redistribute name.	string	Maximum length: 35							
status	Status.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>				Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.
	Option	Description								
	<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.									
metric	Redistribute metric setting.	integer	Minimum value: 0 Maximum value: 16777214	0						
routemap	Route map name.	string	Maximum length: 35							



Parameter	Description	Type	Size	Default
metric-type	Metric type.	option	-	2
	Option	Description		
	1	Type 1.		
	2	Type 2.		

## config summary-address

Parameter	Description	Type	Size	Default						
id	Summary address entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0						
prefix6	IPv6 prefix.	ipv6-network	Not Specified	::/0						
advertise	Enable/disable advertise status.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>disable</td></tr><tr><td><i>enable</i></td><td>enable</td></tr></table>				Option	Description	<i>disable</i>	disable	<i>enable</i>	enable
	Option	Description								
	<i>disable</i>	disable								
<i>enable</i>	enable									
tag	Tag value.	integer	Minimum value: 0 Maximum value: 4294967295	0						

## config router policy

Configure IPv4 routing policies.

```
config router policy
  Description: Configure IPv4 routing policies.
  edit <seq-num>
    set action [deny|permit]
    set comments {var-string}
    set dst <subnet1>, <subnet2>, ...
    set dst-negate [enable|disable]
    set dstaddr <name1>, <name2>, ...
    set end-port {integer}
    set end-source-port {integer}
    set gateway {ipv4-address}
    set input-device <name1>, <name2>, ...
```

```

set input-device-negate [enable|disable]
set internet-service-custom <name1>, <name2>, ...
set internet-service-id <id1>, <id2>, ...
set output-device {string}
set protocol {integer}
set src <subnet1>, <subnet2>, ...
set src-negate [enable|disable]
set srcaddr <name1>, <name2>, ...
set start-port {integer}
set start-source-port {integer}
set status [enable|disable]
set tos {user}
set tos-mask {user}
next
end

```

## config router policy

Parameter	Description	Type	Size	Default						
action	Action of the policy route.	option	-	permit						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>deny</i></td><td>Do not search policy route table.</td></tr><tr><td><i>permit</i></td><td>Use this policy route for forwarding.</td></tr></table>	Option	Description	<i>deny</i>	Do not search policy route table.	<i>permit</i>	Use this policy route for forwarding.			
Option	Description									
<i>deny</i>	Do not search policy route table.									
<i>permit</i>	Use this policy route for forwarding.									
comments	Optional comments.	var-string	Maximum length: 255							
dst <subnet>	Destination IP and mask (x.x.x.x/x). IP and mask.	string	Maximum length: 79							
dst-negate	Enable/disable negating destination address match.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable destination address negation.</td></tr><tr><td><i>disable</i></td><td>Disable destination address negation.</td></tr></table>	Option	Description	<i>enable</i>	Enable destination address negation.	<i>disable</i>	Disable destination address negation.			
Option	Description									
<i>enable</i>	Enable destination address negation.									
<i>disable</i>	Disable destination address negation.									
dstaddr <name>	Destination address name. Address/group name.	string	Maximum length: 79							
end-port	End destination port number.	integer	Minimum value: 0 Maximum value: 65535	65535						
end-source-port	End source port number.	integer	Minimum value: 0 Maximum value: 65535	65535						

Parameter	Description	Type	Size	Default						
gateway	IP address of the gateway.	ipv4-address	Not Specified	0.0.0.0						
input-device <name>	Incoming interface name. Interface name.	string	Maximum length: 79							
input-device-negate	Enable/disable negation of input device match.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable negation of input device match.</td></tr><tr><td>disable</td><td>Disable negation of input device match.</td></tr></table>	Option	Description	enable	Enable negation of input device match.	disable	Disable negation of input device match.			
Option	Description									
enable	Enable negation of input device match.									
disable	Disable negation of input device match.									
internet-service-custom <name>	Custom Destination Internet Service name. Custom Destination Internet Service name.	string	Maximum length: 79							
internet-service-id <id>	Destination Internet Service ID. Destination Internet Service ID.	integer	Minimum value: 0 Maximum value: 4294967295							
output-device	Outgoing interface name.	string	Maximum length: 35							
protocol	Protocol number.	integer	Minimum value: 0 Maximum value: 255	0						
seq-num	Sequence number.	integer	Minimum value: 1 Maximum value: 65535	0						
src <subnet>	Source IP and mask (x.x.x.x/x). IP and mask.	string	Maximum length: 79							
src-negate	Enable/disable negating source address match.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable source address negation.</td></tr><tr><td>disable</td><td>Disable source address negation.</td></tr></table>	Option	Description	enable	Enable source address negation.	disable	Disable source address negation.			
Option	Description									
enable	Enable source address negation.									
disable	Disable source address negation.									
srcaddr <name>	Source address name. Address/group name.	string	Maximum length: 79							

Parameter	Description	Type	Size	Default						
start-port	Start destination port number.	integer	Minimum value: 0 Maximum value: 65535	0						
start-source-port	Start source port number.	integer	Minimum value: 0 Maximum value: 65535	0						
status	Enable/disable this policy route.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable this policy route.</td></tr><tr><td><i>disable</i></td><td>Disable this policy route.</td></tr></table>				Option	Description	<i>enable</i>	Enable this policy route.	<i>disable</i>	Disable this policy route.
	Option	Description								
	<i>enable</i>	Enable this policy route.								
<i>disable</i>	Disable this policy route.									
tos	Type of service bit pattern.	user	Not Specified							
tos-mask	Type of service evaluated bits.	user	Not Specified							

## config router policy6

Configure IPv6 routing policies.

```

config router policy6
    Description: Configure IPv6 routing policies.
    edit <seq-num>
        set comments {var-string}
        set dst {ipv6-network}
        set end-port {integer}
        set gateway {ipv6-address}
        set input-device <name1>, <name2>, ...
        set output-device {string}
        set protocol {integer}
        set src {ipv6-network}
        set start-port {integer}
        set status [enable|disable]
        set tos {user}
        set tos-mask {user}
    next
end

```

## config router policy6

Parameter	Description	Type	Size	Default
comments	Optional comments.	var-string	Maximum length: 255	

Parameter	Description	Type	Size	Default						
dst	Destination IPv6 prefix.	ipv6-network	Not Specified	::/0						
end-port	End destination port number.	integer	Minimum value: 1 Maximum value: 65535	65535						
gateway	IPv6 address of the gateway.	ipv6-address	Not Specified	::						
input-device <name>	Incoming interface name. Interface name.	string	Maximum length: 79							
output-device	Outgoing interface name.	string	Maximum length: 35							
protocol	Protocol number.	integer	Minimum value: 0 Maximum value: 255	0						
seq-num	Sequence number.	integer	Minimum value: 1 Maximum value: 65535	0						
src	Source IPv6 prefix.	ipv6-network	Not Specified	::/0						
start-port	Start destination port number.	integer	Minimum value: 1 Maximum value: 65535	1						
status	Enable/disable this policy route.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable this policy route.</td></tr><tr><td><i>disable</i></td><td>Disable this policy route.</td></tr></table>				Option	Description	<i>enable</i>	Enable this policy route.	<i>disable</i>	Disable this policy route.
Option	Description									
<i>enable</i>	Enable this policy route.									
<i>disable</i>	Disable this policy route.									
tos	Type of service bit pattern.	user	Not Specified							
tos-mask	Type of service evaluated bits.	user	Not Specified							

## config router prefix-list

Configure IPv4 prefix lists.

```
config router prefix-list
  Description: Configure IPv4 prefix lists.
  edit <name>
    set comments {string}
    config rule
      Description: IPv4 prefix list rule.
      edit <id>
        set action [permit|deny]
        set prefix {user}
        set ge {integer}
        set le {integer}
      next
    end
  next
end
```

## config router prefix-list

Parameter	Description	Type	Size	Default
comments	Comment.	string	Maximum length: 127	
name	Name.	string	Maximum length: 35	

## config rule

Parameter	Description	Type	Size	Default
id	Rule ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
action	Permit or deny this IP address and netmask prefix.	option	-	permit
		Option	Description	
		<i>permit</i>	Allow or permit packets that match this rule.	
		<i>deny</i>	Deny packets that match this rule.	
prefix	IPv4 prefix to define regular filter criteria, such as "any" or subnets.	user	Not Specified	0.0.0.0 0.0.0.0

Parameter	Description	Type	Size	Default
ge	Minimum prefix length to be matched.	integer	Minimum value: 0 Maximum value: 32	
le	Maximum prefix length to be matched.	integer	Minimum value: 0 Maximum value: 32	

## config router prefix-list6

Configure IPv6 prefix lists.

```

config router prefix-list6
    Description: Configure IPv6 prefix lists.
    edit <name>
        set comments {string}
        config rule
            Description: IPv6 prefix list rule.
            edit <id>
                set action [permit|deny]
                set prefix6 {user}
                set ge {integer}
                set le {integer}
                set flags {integer}
            next
        end
    next
end

```

## config router prefix-list6

Parameter	Description	Type	Size	Default
comments	Comment.	string	Maximum length: 127	
name	Name.	string	Maximum length: 35	

## config rule

Parameter	Description	Type	Size	Default
id	Rule ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
action	Permit or deny packets that match this rule.	option	-	permit
	Option	Description		
	permit	Allow or permit packets that match this rule.		
	deny	Deny packets that match this rule.		
prefix6	IPv6 prefix to define regular filter criteria, such as "any" or subnets.	user	Not Specified	
ge	Minimum prefix length to be matched.	integer	Minimum value: 0 Maximum value: 128	
le	Maximum prefix length to be matched.	integer	Minimum value: 0 Maximum value: 128	
flags	Flags.	integer	Minimum value: 0 Maximum value: 4294967295	0

## config router rip

Configure RIP.

```
config router rip
  Description: Configure RIP.
  set default-information-originate [enable|disable]
  set default-metric {integer}
  config distance
    Description: Distance.
    edit <id>
      set prefix {ipv4-classnet-any}
      set distance {integer}
      set access-list {string}
    next
  end
config distribute-list
```



```

    Description: Distribute list.
    edit <id>
        set status [enable|disable]
        set direction [in|out]
        set listname {string}
        set interface {string}
    next
end
set garbage-timer {integer}
config interface
    Description: RIP interface configuration.
    edit <name>
        set auth-keychain {string}
        set auth-mode [none|text|...]
        set auth-string {password}
        set receive-version {option1}, {option2}, ...
        set send-version {option1}, {option2}, ...
        set send-version2-broadcast [disable|enable]
        set split-horizon-status [enable|disable]
        set split-horizon [poisoned|regular]
        set flags {integer}
    next
end
set max-out-metric {integer}
config neighbor
    Description: Neighbor.
    edit <id>
        set ip {ipv4-address}
    next
end
config network
    Description: Network.
    edit <id>
        set prefix {ipv4-classnet}
    next
end
config offset-list
    Description: Offset list.
    edit <id>
        set status [enable|disable]
        set direction [in|out]
        set access-list {string}
        set offset {integer}
        set interface {string}
    next
end
set passive-interface <name1>, <name2>, ...
config redistribute
    Description: Redistribute configuration.
    edit <name>
        set status [enable|disable]
        set metric {integer}
        set routemap {string}
    next
end
set timeout-timer {integer}

```

```

    set update-timer {integer}
    set version [1|2]
end

```

## config router rip

Parameter	Description	Type	Size	Default						
default-information-originate	Enable/disable generation of default route.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
default-metric	Default metric.	integer	Minimum value: 1 Maximum value: 16	1						
garbage-timer	Garbage timer in seconds.	integer	Minimum value: 5 Maximum value: 2147483647	120						
max-out-metric	Maximum metric allowed to output(0 means 'not set').	integer	Minimum value: 0 Maximum value: 15	0						
passive-interface <name>	Passive interface configuration. Passive interface name.	string	Maximum length: 79							
timeout-timer	Timeout timer in seconds.	integer	Minimum value: 5 Maximum value: 2147483647	180						
update-timer	Update timer in seconds.	integer	Minimum value: 1 Maximum value: 2147483647	30						
version	RIP version.	option	-	2						

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	1	Version 1.		
	2	Version 2.		

### config distance

Parameter	Description	Type	Size	Default
id	Distance ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
prefix	Distance prefix.	ipv4-classnet-any	Not Specified	0.0.0.0 0.0.0.0
distance	Distance.	integer	Minimum value: 1 Maximum value: 255	0
access-list	Access list for route destination.	string	Maximum length: 35	

### config distribute-list

Parameter	Description	Type	Size	Default
id	Distribute list ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
status	Status.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
direction	Distribute list direction.	option	-	out

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>in</i>	Filter incoming packets.		
	<i>out</i>	Filter outgoing packets.		
listname	Distribute access/prefix list name.	string	Maximum length: 35	
interface	Distribute list interface name.	string	Maximum length: 15	

### config interface

Parameter	Description	Type	Size	Default
name	Interface name.	string	Maximum length: 35	
auth-keychain	Authentication key-chain name.	string	Maximum length: 35	
auth-mode	Authentication mode.	option	-	none
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	None.		
	<i>text</i>	Text.		
	<i>md5</i>	MD5.		
auth-string	Authentication string/password.	password	Not Specified	
receive-version	Receive version.	option	-	
	<b>Option</b>	<b>Description</b>		
	<i>1</i>	Version 1.		
	<i>2</i>	Version 2.		
send-version	Send version.	option	-	
	<b>Option</b>	<b>Description</b>		
	<i>1</i>	Version 1.		
	<i>2</i>	Version 2.		

Parameter	Description	Type	Size	Default
send-version2-broadcast	Enable/disable broadcast version 1 compatible packets.	option	-	disable
	Option	Description		
	disable	Disable broadcasting.		
	enable	Enable broadcasting.		
split-horizon-status	Enable/disable split horizon.	option	-	enable
	Option	Description		
	enable	Enable setting.		
	disable	Disable setting.		
split-horizon	Enable/disable split horizon.	option	-	poisoned
	Option	Description		
	poisoned	Poisoned.		
	regular	Regular.		
flags	Flags.	integer	Minimum value: 0 Maximum value: 255	8

### config neighbor

Parameter	Description	Type	Size	Default
id	Neighbor entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
ip	IP address.	ipv4-address	Not Specified	0.0.0.0

## config network

Parameter	Description	Type	Size	Default
id	Network entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
prefix	Network prefix.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0

## config offset-list

Parameter	Description	Type	Size	Default
id	Offset-list ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
status	Status.	option	-	enable
	Option	Description		
	enable	Enable setting.		
	disable	Disable setting.		
direction	Offset list direction.	option	-	out
	Option	Description		
	in	Filter incoming packets.		
	out	Filter outgoing packets.		
access-list	Access list name.	string	Maximum length: 35	
offset	Offset.	integer	Minimum value: 1 Maximum value: 16	0
interface	Interface name.	string	Maximum length: 15	

## config redistribute

Parameter	Description	Type	Size	Default
name	Redistribute name.	string	Maximum length: 35	
status	Status.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
metric	Redistribute metric setting.	integer	Minimum value: 1 Maximum value: 16	0
route-map	Route map name.	string	Maximum length: 35	

## config router ripng

Configure RIPng.

```
config router ripng
  Description: Configure RIPng.
  config aggregate-address
    Description: Aggregate address.
    edit <id>
      set prefix6 {ipv6-prefix}
    next
  end
  set default-information-originate [enable|disable]
  set default-metric {integer}
  config distance
    Description: Distance.
    edit <id>
      set distance {integer}
      set prefix6 {ipv6-prefix}
      set access-list6 {string}
    next
  end
  config distribute-list
    Description: Distribute list.
    edit <id>
      set status [enable|disable]
      set direction [in|out]
      set listname {string}
      set interface {string}
    next
  end
  set garbage-timer {integer}
```

```

config interface
    Description: RIPng interface configuration.
    edit <name>
        set split-horizon-status [enable|disable]
        set split-horizon [poisoned|regular]
        set flags {integer}
    next
end
set max-out-metric {integer}
config neighbor
    Description: Neighbor.
    edit <id>
        set ip6 {ipv6-address}
        set interface {string}
    next
end
config network
    Description: Network.
    edit <id>
        set prefix {ipv6-prefix}
    next
end
config offset-list
    Description: Offset list.
    edit <id>
        set status [enable|disable]
        set direction [in|out]
        set access-list6 {string}
        set offset {integer}
        set interface {string}
    next
end
set passive-interface <name1>, <name2>, ...
config redistribute
    Description: Redistribute configuration.
    edit <name>
        set status [enable|disable]
        set metric {integer}
        set routemap {string}
    next
end
set timeout-timer {integer}
set update-timer {integer}
end

```

## config router ripng

Parameter	Description	Type	Size	Default
default-information-originate	Enable/disable generation of default route.	option	-	disable



Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
	Option	Description								
	<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.									
default-metric	Default metric.	integer	Minimum value: 1 Maximum value: 16	1						
garbage-timer	Garbage timer.	integer	Minimum value: 5 Maximum value: 2147483647	120						
max-out-metric	Maximum metric allowed to output(0 means 'not set').	integer	Minimum value: 0 Maximum value: 15	0						
passive-interface <name>	Passive interface configuration. Passive interface name.	string	Maximum length: 79							
timeout-timer	Timeout timer.	integer	Minimum value: 5 Maximum value: 2147483647	180						
update-timer	Update timer.	integer	Minimum value: 5 Maximum value: 2147483647	30						

### config aggregate-address

Parameter	Description	Type	Size	Default
id	Aggregate address entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
prefix6	Aggregate address prefix.	ipv6-prefix	Not Specified	::/0

## config distance

Parameter	Description	Type	Size	Default
id	Distance ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
distance	Distance.	integer	Minimum value: 1 Maximum value: 255	0
prefix6	Distance prefix6.	ipv6-prefix	Not Specified	::/0
access-list6	Access list for route destination.	string	Maximum length: 35	

## config distribute-list

Parameter	Description	Type	Size	Default						
id	Distribute list ID.	integer	Minimum value: 0 Maximum value: 4294967295	0						
status	Status.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>				Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.
	Option	Description								
	<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.									
direction	Distribute list direction.	option	-	out						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>in</i></td><td>Filter incoming packets.</td></tr><tr><td><i>out</i></td><td>Filter outgoing packets.</td></tr></table>				Option	Description	<i>in</i>	Filter incoming packets.	<i>out</i>	Filter outgoing packets.
	Option	Description								
	<i>in</i>	Filter incoming packets.								
<i>out</i>	Filter outgoing packets.									
listname	Distribute access/prefix list name.	string	Maximum length: 35							
interface	Distribute list interface name.	string	Maximum length: 15							

## config interface

Parameter	Description	Type	Size	Default
name	Interface name.	string	Maximum length: 35	
split-horizon-status	Enable/disable split horizon.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
split-horizon	Enable/disable split horizon.	option	-	poisoned
	<b>Option</b>	<b>Description</b>		
	<i>poisoned</i>	Poisoned.		
	<i>regular</i>	Regular.		
flags	Flags.	integer	Minimum value: 0 Maximum value: 255	8

## config neighbor

Parameter	Description	Type	Size	Default
id	Neighbor entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
ip6	IPv6 link-local address.	ipv6-address	Not Specified	::
interface	Interface name.	string	Maximum length: 15	

## config network

Parameter	Description	Type	Size	Default
id	Network entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
prefix	Network IPv6 link-local prefix.	ipv6-prefix	Not Specified	::/0

## config offset-list

Parameter	Description	Type	Size	Default						
id	Offset-list ID.	integer	Minimum value: 0 Maximum value: 4294967295	0						
status	Status.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>				Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.
	Option	Description								
	<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.									
direction	Offset list direction.	option	-	out						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>in</i></td><td>Filter incoming packets.</td></tr><tr><td><i>out</i></td><td>Filter outgoing packets.</td></tr></table>				Option	Description	<i>in</i>	Filter incoming packets.	<i>out</i>	Filter outgoing packets.
	Option	Description								
	<i>in</i>	Filter incoming packets.								
<i>out</i>	Filter outgoing packets.									
access-list6	IPv6 access list name.	string	Maximum length: 35							
offset	Offset.	integer	Minimum value: 1 Maximum value: 16	0						
interface	Interface name.	string	Maximum length: 15							

## config redistribute

Parameter	Description	Type	Size	Default
name	Redistribute name.	string	Maximum length: 35	
status	Status.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
metric	Redistribute metric setting.	integer	Minimum value: 1 Maximum value: 16	0
route-map	Route map name.	string	Maximum length: 35	

## config router route-map

Configure route maps.

```
config router route-map
  Description: Configure route maps.
  edit <name>
    set comments {string}
    config rule
      Description: Rule.
      edit <id>
        set action [permit|deny]
        set match-as-path {string}
        set match-community {string}
        set match-community-exact [enable|disable]
        set match-origin [none|egp|...]
        set match-interface {string}
        set match-ip-address {string}
        set match-ip6-address {string}
        set match-ip-nexthop {string}
        set match-ip6-nexthop {string}
        set match-metric {integer}
        set match-route-type [external-type1|external-type2|...]
        set match-tag {integer}
        set match-vrf {integer}
        set set-aggregator-as {integer}
        set set-aggregator-ip {ipv4-address-any}
        set set-aspath-action [prepend|replace]
        set set-aspath <as1>, <as2>, ...
        set set-atomic-aggregate [enable|disable]
        set set-community-delete {string}
        set set-community <community1>, <community2>, ...
```

```

        set set-community-additive [enable|disable]
        set set-dampening-reachability-half-life {integer}
        set set-dampening-reuse {integer}
        set set-dampening-suppress {integer}
        set set-dampening-max-suppress {integer}
        set set-dampening-unreachability-half-life {integer}
        set set-extcommunity-rt <community1>, <community2>, ...
        set set-extcommunity-soo <community1>, <community2>, ...
        set set-ip-nexthop {ipv4-address}
        set set-ip6-nexthop {ipv6-address}
        set set-ip6-nexthop-local {ipv6-address}
        set set-local-preference {integer}
        set set-metric {integer}
        set set-metric-type [external-type1|external-type2|...]
        set set-originator-id {ipv4-address-any}
        set set-origin [none|egp|...]
        set set-tag {integer}
        set set-weight {integer}
        set set-route-tag {integer}
    next
end
next
end

```

## config router route-map

Parameter	Description	Type	Size	Default
comments	Optional comments.	string	Maximum length: 127	
name	Name.	string	Maximum length: 35	

## config rule

Parameter	Description	Type	Size	Default
id	Rule ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
action	Action.	option	-	permit
	Option	Description		
	permit	Permit.		
	deny	Deny.		

Parameter	Description	Type	Size	Default										
match-as-path	Match BGP AS path list.	string	Maximum length: 35											
match-community	Match BGP community list.	string	Maximum length: 35											
match-community-exact	Enable/disable exact matching of communities.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable exact matching of communities.</td></tr><tr><td><i>disable</i></td><td>Disable exact matching of communities.</td></tr></table>	Option	Description	<i>enable</i>	Enable exact matching of communities.	<i>disable</i>	Disable exact matching of communities.							
Option	Description													
<i>enable</i>	Enable exact matching of communities.													
<i>disable</i>	Disable exact matching of communities.													
match-origin	Match BGP origin code.	option	-	none										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>None.</td></tr><tr><td><i>egp</i></td><td>Remote EGP.</td></tr><tr><td><i>igp</i></td><td>Local IGP.</td></tr><tr><td><i>incomplete</i></td><td>Unknown heritage.</td></tr></table>	Option	Description	<i>none</i>	None.	<i>egp</i>	Remote EGP.	<i>igp</i>	Local IGP.	<i>incomplete</i>	Unknown heritage.			
Option	Description													
<i>none</i>	None.													
<i>egp</i>	Remote EGP.													
<i>igp</i>	Local IGP.													
<i>incomplete</i>	Unknown heritage.													
match-interface	Match interface configuration.	string	Maximum length: 15											
match-ip-address	Match IP address permitted by access-list or prefix-list.	string	Maximum length: 35											
match-ip6-address	Match IPv6 address permitted by access-list6 or prefix-list6.	string	Maximum length: 35											
match-ip-nexthop	Match next hop IP address passed by access-list or prefix-list.	string	Maximum length: 35											
match-ip6-nexthop	Match next hop IPv6 address passed by access-list6 or prefix-list6.	string	Maximum length: 35											
match-metric	Match metric for redistribute routes.	integer	Minimum value: 0 Maximum value: 4294967295											
match-route-type	Match route type.	option	-											
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>external-type1</i></td><td>External type 1.</td></tr></table>	Option	Description	<i>external-type1</i>	External type 1.									
Option	Description													
<i>external-type1</i>	External type 1.													

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>external-type2</i></td><td>External type 2.</td></tr><tr><td><i>none</i></td><td>No type specified.</td></tr></table>				Option	Description	<i>external-type2</i>	External type 2.	<i>none</i>	No type specified.
	Option	Description								
	<i>external-type2</i>	External type 2.								
<i>none</i>	No type specified.									
match-tag	Match tag.	integer	Minimum value: 0 Maximum value: 4294967295							
match-vrf	Match VRF ID.	integer	Minimum value: 0 Maximum value: 31							
set-aggregator-as	BGP aggregator AS.	integer	Minimum value: 0 Maximum value: 4294967295	0						
set-aggregator-ip	BGP aggregator IP.	ipv4-address-any	Not Specified	0.0.0.0						
set-aspath-action	Specify preferred action of set-aspath.	option	-	prepend						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>prepend</i></td><td>Prepend.</td></tr><tr><td><i>replace</i></td><td>Replace.</td></tr></table>				Option	Description	<i>prepend</i>	Prepend.	<i>replace</i>	Replace.
	Option	Description								
	<i>prepend</i>	Prepend.								
<i>replace</i>	Replace.									
set-aspath <as>	Prepend BGP AS path attribute. AS number (0 - 4294967295). Use quotes for repeating numbers, For example, "1 1 2".	string	Maximum length: 79							
set-atomic-aggregate	Enable/disable BGP atomic aggregate attribute.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable BGP atomic aggregate attribute.</td></tr><tr><td><i>disable</i></td><td>Disable BGP atomic aggregate attribute.</td></tr></table>				Option	Description	<i>enable</i>	Enable BGP atomic aggregate attribute.	<i>disable</i>	Disable BGP atomic aggregate attribute.
	Option	Description								
	<i>enable</i>	Enable BGP atomic aggregate attribute.								
<i>disable</i>	Disable BGP atomic aggregate attribute.									
set-community-delete	Delete communities matching community list.	string	Maximum length: 35							



Parameter	Description	Type	Size	Default						
set-community <community>	BGP community attribute. Attribute: AA AA:NN internet local-AS no-advertise no-export.	string	Maximum length: 79							
set-community-additive	Enable/disable adding set-community to existing community.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable adding set-community to existing community.</td></tr><tr><td>disable</td><td>Disable adding set-community to existing community.</td></tr></table>				Option	Description	enable	Enable adding set-community to existing community.	disable	Disable adding set-community to existing community.
Option	Description									
enable	Enable adding set-community to existing community.									
disable	Disable adding set-community to existing community.									
set-dampening-reachability-half-life	Reachability half-life time for the penalty.	integer	Minimum value: 0 Maximum value: 45	0						
set-dampening-reuse	Value to start reusing a route.	integer	Minimum value: 0 Maximum value: 20000	0						
set-dampening-suppress	Value to start suppressing a route.	integer	Minimum value: 0 Maximum value: 20000	0						
set-dampening-max-suppress	Maximum duration to suppress a route.	integer	Minimum value: 0 Maximum value: 255	0						
set-dampening-unreachability-half-life	Unreachability Half-life time for the penalty.	integer	Minimum value: 0 Maximum value: 45	0						
set-extcommunity-rt <community>	Route Target extended community. AA:NN.	string	Maximum length: 79							
set-extcommunity-soo <community>	Site-of-Origin extended community. Community (format = AA:NN).	string	Maximum length: 79							
set-ip-nexthop	IP address of next hop.	ipv4- address	Not Specified							

Parameter	Description	Type	Size	Default
set-ip6-nexthop	IPv6 global address of next hop.	ipv6-address	Not Specified	
set-ip6-nexthop-local	IPv6 local address of next hop.	ipv6-address	Not Specified	
set-local-preference	BGP local preference path attribute.	integer	Minimum value: 0 Maximum value: 4294967295	
set-metric	Metric value.	integer	Minimum value: 0 Maximum value: 4294967295	
set-metric-type	Metric type.	option	-	
	Option	Description		
	external-type1	External type 1.		
	external-type2	External type 2.		
	none	No type specified.		
set-originator-id	BGP originator ID attribute.	ipv4-address-any	Not Specified	
set-origin	BGP origin code.	option	-	none
	Option	Description		
	none	None.		
	egp	Remote EGP.		
	igp	Local IGP.		
	incomplete	Unknown heritage.		
set-tag	Tag value.	integer	Minimum value: 0 Maximum value: 4294967295	

Parameter	Description	Type	Size	Default
set-weight	BGP weight for routing table.	integer	Minimum value: 0 Maximum value: 4294967295	
set-route-tag	Route tag for routing table.	integer	Minimum value: 0 Maximum value: 4294967295	

## config router setting

Configure router settings.

```
config router setting
    Description: Configure router settings.
    set hostname {string}
    set show-filter {string}
end
```

## config router setting

Parameter	Description	Type	Size	Default
hostname	Hostname for this virtual domain router.	string	Maximum length: 14	
show-filter	Prefix-list as filter for showing routes.	string	Maximum length: 35	

## config router static

Configure IPv4 static routing tables.

```
config router static
    Description: Configure IPv4 static routing tables.
    edit <seq-num>
        set bfd [enable|disable]
        set blackhole [enable|disable]
        set comment {var-string}
        set device {string}
        set distance {integer}
        set dst {ipv4-classnet}
        set dstaddr {string}
        set dynamic-gateway [enable|disable]
        set gateway {ipv4-address}
        set internet-service {integer}
```

```

        set internet-service-custom {string}
        set link-monitor-exempt [enable|disable]
        set priority {integer}
        set sdwan-zone <name1>, <name2>, ...
        set src {ipv4-classnet}
        set status [enable|disable]
        set vrf {integer}
        set weight {integer}
    next
end

```

## config router static

Parameter	Description	Type	Size	Default						
bfd	Enable/disable Bidirectional Forwarding Detection (BFD).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Bidirectional Forwarding Detection (BFD).</td></tr><tr><td><i>disable</i></td><td>Disable Bidirectional Forwarding Detection (BFD).</td></tr></table>	Option	Description	<i>enable</i>	Enable Bidirectional Forwarding Detection (BFD).	<i>disable</i>	Disable Bidirectional Forwarding Detection (BFD).			
Option	Description									
<i>enable</i>	Enable Bidirectional Forwarding Detection (BFD).									
<i>disable</i>	Disable Bidirectional Forwarding Detection (BFD).									
blackhole	Enable/disable black hole.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable black hole.</td></tr><tr><td><i>disable</i></td><td>Disable black hole.</td></tr></table>	Option	Description	<i>enable</i>	Enable black hole.	<i>disable</i>	Disable black hole.			
Option	Description									
<i>enable</i>	Enable black hole.									
<i>disable</i>	Disable black hole.									
comment	Optional comments.	var-string	Maximum length: 255							
device	Gateway out interface or tunnel.	string	Maximum length: 35							
distance	Administrative distance.	integer	Minimum value: 1 Maximum value: 255	10						
dst	Destination IP and mask for this route.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0						
dstaddr	Name of firewall address or address group.	string	Maximum length: 79							
dynamic-gateway	Enable use of dynamic gateway retrieved from a DHCP or PPP server.	option	-	disable						

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable dynamic gateway.</td></tr><tr><td><i>disable</i></td><td>Disable dynamic gateway.</td></tr></table>	Option	Description	<i>enable</i>	Enable dynamic gateway.	<i>disable</i>	Disable dynamic gateway.			
	Option	Description								
	<i>enable</i>	Enable dynamic gateway.								
<i>disable</i>	Disable dynamic gateway.									
gateway	Gateway IP for this route.	ipv4-address	Not Specified	0.0.0.0						
internet-service	Application ID in the Internet service database.	integer	Minimum value: 0 Maximum value: 4294967295	0						
internet-service-custom	Application name in the Internet service custom database.	string	Maximum length: 64							
link-monitor-exempt	Enable/disable withdrawal of this static route when link monitor or health check is down.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Keep this static route when link monitor or health check is down.</td></tr><tr><td><i>disable</i></td><td>Withdraw this static route when link monitor or health check is down. (default)</td></tr></table>	Option	Description	<i>enable</i>	Keep this static route when link monitor or health check is down.	<i>disable</i>	Withdraw this static route when link monitor or health check is down. (default)			
	Option	Description								
	<i>enable</i>	Keep this static route when link monitor or health check is down.								
<i>disable</i>	Withdraw this static route when link monitor or health check is down. (default)									
priority	Administrative priority.	integer	Minimum value: 1 Maximum value: 65535	1						
sdwan-zone <name>	Choose SD-WAN Zone. SD-WAN zone name.	string	Maximum length: 79							
seq-num	Sequence number.	integer	Minimum value: 0 Maximum value: 4294967295	0						
src	Source prefix for this route.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0						
status	Enable/disable this static route.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable static route.</td></tr><tr><td><i>disable</i></td><td>Disable static route.</td></tr></table>	Option	Description	<i>enable</i>	Enable static route.	<i>disable</i>	Disable static route.			
	Option	Description								
	<i>enable</i>	Enable static route.								
<i>disable</i>	Disable static route.									

Parameter	Description	Type	Size	Default
vrf	Virtual Routing Forwarding ID.	integer	Minimum value: 0 Maximum value: 31	0
weight	Administrative weight.	integer	Minimum value: 0 Maximum value: 255	0

## config router static6

Configure IPv6 static routing tables.

```

config router static6
    Description: Configure IPv6 static routing tables.
    edit <seq-num>
        set bfd [enable|disable]
        set blackhole [enable|disable]
        set comment {var-string}
        set device {string}
        set devindex {integer}
        set distance {integer}
        set dst {ipv6-network}
        set dynamic-gateway [enable|disable]
        set gateway {ipv6-address}
        set link-monitor-exempt [enable|disable]
        set priority {integer}
        set sdwan-zone <name1>, <name2>, ...
        set status [enable|disable]
        set vrf {integer}
    next
end

```

## config router static6

Parameter	Description	Type	Size	Default						
bfd	Enable/disable Bidirectional Forwarding Detection (BFD).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Bidirectional Forwarding Detection (BFD).</td></tr><tr><td><i>disable</i></td><td>Disable Bidirectional Forwarding Detection (BFD).</td></tr></table>	Option	Description	<i>enable</i>	Enable Bidirectional Forwarding Detection (BFD).	<i>disable</i>	Disable Bidirectional Forwarding Detection (BFD).			
Option	Description									
<i>enable</i>	Enable Bidirectional Forwarding Detection (BFD).									
<i>disable</i>	Disable Bidirectional Forwarding Detection (BFD).									
blackhole	Enable/disable black hole.	option	-	disable						

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable black hole.</td></tr><tr><td><i>disable</i></td><td>Disable black hole.</td></tr></table>				Option	Description	<i>enable</i>	Enable black hole.	<i>disable</i>	Disable black hole.
	Option	Description								
	<i>enable</i>	Enable black hole.								
<i>disable</i>	Disable black hole.									
comment	Optional comments.	var-string	Maximum length: 255							
device	Gateway out interface or tunnel.	string	Maximum length: 35							
devindex	Device index.	integer	Minimum value: 0 Maximum value: 4294967295	0						
distance	Administrative distance.	integer	Minimum value: 1 Maximum value: 255	10						
dst	Destination IPv6 prefix.	ipv6-network	Not Specified	::/0						
dynamic-gateway	Enable use of dynamic gateway retrieved from Router Advertisement (RA).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable dynamic gateway.</td></tr><tr><td><i>disable</i></td><td>Disable dynamic gateway.</td></tr></table>				Option	Description	<i>enable</i>	Enable dynamic gateway.	<i>disable</i>	Disable dynamic gateway.
	Option	Description								
	<i>enable</i>	Enable dynamic gateway.								
<i>disable</i>	Disable dynamic gateway.									
gateway	IPv6 address of the gateway.	ipv6-address	Not Specified	::						
link-monitor-exempt	Enable/disable withdrawal of this static route when link monitor or health check is down.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Keep this static route when link monitor or health check is down.</td></tr><tr><td><i>disable</i></td><td>Withdraw this static route when link monitor or health check is down. (default)</td></tr></table>				Option	Description	<i>enable</i>	Keep this static route when link monitor or health check is down.	<i>disable</i>	Withdraw this static route when link monitor or health check is down. (default)
	Option	Description								
	<i>enable</i>	Keep this static route when link monitor or health check is down.								
<i>disable</i>	Withdraw this static route when link monitor or health check is down. (default)									
priority	Administrative priority.	integer	Minimum value: 1 Maximum value: 65535	1024						

Parameter	Description	Type	Size	Default
sdwan-zone <name>	Choose SD-WAN Zone. SD-WAN zone name.	string	Maximum length: 79	
seq-num	Sequence number.	integer	Minimum value: 0 Maximum value: 4294967295	0
status	Enable/disable this static route.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable static route.		
	<i>disable</i>	Disable static route.		
vrf	Virtual Routing Forwarding ID.	integer	Minimum value: 0 Maximum value: 31	0



## sctp-filter

This section includes syntax for the following commands:

- [config sctp-filter profile on page 893](#)

### config sctp-filter profile

Configure SCTP filter profiles.

```
config sctp-filter profile
  Description: Configure SCTP filter profiles.
  edit <name>
    set comment {var-string}
    config ppid-filters
      Description: PPID filters list.
      edit <id>
        set ppid {integer}
        set action [pass|reset|...]
        set comment {var-string}
      next
    end
  next
end
```

### config sctp-filter profile

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 255	
name	Profile name.	string	Maximum length: 35	

### config ppid-filters

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0

Parameter	Description	Type	Size	Default
ppid	Payload protocol identifier.	integer	Minimum value: 0 Maximum value: 4294967295	
action	Action taken when PPID is matched.	option	-	reset
	<b>Option</b>	<b>Description</b>		
	<i>pass</i>	Pass data chunk.		
	<i>reset</i>	Reset SCTP session.		
	<i>replace</i>	Replace data chunk.		
comment	Comment.	var-string	Maximum length: 255	

# ssh-filter

This section includes syntax for the following commands:

- [config ssh-filter profile on page 895](#)

## config ssh-filter profile

Configure SSH filter profile.

```
config ssh-filter profile
  Description: Configure SSH filter profile.
  edit <name>
    set block {option1}, {option2}, ...
    set default-command-log [enable|disable]
    set log {option1}, {option2}, ...
    config shell-commands
      Description: SSH command filter.
      edit <id>
        set type [simple|regex]
        set pattern {string}
        set action [block|allow]
        set log [enable|disable]
        set alert [enable|disable]
        set severity [low|medium|...]
      next
    end
  next
end
```

## config ssh-filter profile

Parameter	Description	Type	Size	Default
block	SSH blocking options.			
	Option	Description		
	x11	X server forwarding.		
	shell	SSH shell.		
	exec	SSH execution.		
	port-forward	Port forwarding.		
	tun-forward	Tunnel forwarding.		
	sftp	SFTP.		

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>scp</i>	SCP.		
	<i>unknown</i>	Unknown channel.		
default-command-log	Enable/disable logging unmatched shell commands.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable log unmatched shell commands.		
	<i>disable</i>	Disable log unmatched shell commands.		
log	SSH logging options.	option	-	
	<b>Option</b>	<b>Description</b>		
	<i>x11</i>	X server forwarding.		
	<i>shell</i>	SSH shell.		
	<i>exec</i>	SSH execution.		
	<i>port-forward</i>	Port forwarding.		
	<i>tun-forward</i>	Tunnel forwarding.		
	<i>sftp</i>	SFTP.		
	<i>scp</i>	SCP.		
	<i>unknown</i>	Unknown channel.		
name	SSH filter profile name.	string	Maximum length: 35	

## config shell-commands

Parameter	Description	Type	Size	Default
id	Id.	integer	Minimum value: 0 Maximum value: 4294967295	0
type	Matching type.	option	-	simple
	<b>Option</b>	<b>Description</b>		
	<i>simple</i>	Match single command.		

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>regex</i>	Match command line using regular expression.		
pattern	SSH shell command pattern.	string	Maximum length: 128	
action	Action to take for SSH shell command matches.	option	-	block
	<b>Option</b>	<b>Description</b>		
	<i>block</i>	Block the SSH shell command.		
	<i>allow</i>	Allow the SSH shell command.		
log	Enable/disable logging.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable logging.		
	<i>disable</i>	Disable logging.		
alert	Enable/disable alert.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable alert.		
	<i>disable</i>	Disable alert.		
severity	Log severity.	option	-	medium
	<b>Option</b>	<b>Description</b>		
	<i>low</i>	Severity low.		
	<i>medium</i>	Severity medium.		
	<i>high</i>	Severity high.		
	<i>critical</i>	Severity critical.		

## switch-controller

This section includes syntax for the following commands:

- [config switch-controller 802-1X-settings on page 899](#)
- [config switch-controller auto-config custom on page 901](#)
- [config switch-controller auto-config default on page 902](#)
- [config switch-controller auto-config policy on page 903](#)
- [config switch-controller custom-command on page 905](#)
- [config switch-controller dsl policy on page 906](#)
- [config switch-controller dynamic-port-policy on page 909](#)
- [config switch-controller flow-tracking on page 912](#)
- [config switch-controller fortilink-settings on page 915](#)
- [config switch-controller global on page 917](#)
- [config switch-controller igmp-snooping on page 921](#)
- [config switch-controller initial-config template on page 923](#)
- [config switch-controller initial-config vlans on page 925](#)
- [config switch-controller lldp-profile on page 926](#)
- [config switch-controller lldp-settings on page 930](#)
- [config switch-controller location on page 932](#)
- [config switch-controller mac-policy on page 937](#)
- [config switch-controller managed-switch on page 939](#)
- [config switch-controller network-monitor-settings on page 974](#)
- [config switch-controller ptp policy on page 975](#)
- [config switch-controller ptp settings on page 976](#)
- [config switch-controller qos dot1p-map on page 977](#)
- [config switch-controller qos ip-dscp-map on page 981](#)
- [config switch-controller qos qos-policy on page 984](#)
- [config switch-controller qos queue-policy on page 985](#)
- [config switch-controller quarantine on page 988](#)
- [config switch-controller remote-log on page 989](#)
- [config switch-controller security-policy 802-1X on page 992](#)
- [config switch-controller security-policy local-access on page 995](#)
- [config switch-controller sflow on page 997](#)
- [config switch-controller snmp-community on page 998](#)
- [config switch-controller snmp-sysinfo on page 1001](#)
- [config switch-controller snmp-trap-threshold on page 1002](#)
- [config switch-controller snmp-user on page 1004](#)
- [config switch-controller storm-control-policy on page 1006](#)
- [config switch-controller storm-control on page 1008](#)
- [config switch-controller stp-instance on page 1010](#)

- [config switch-controller stp-settings on page 1011](#)
- [config switch-controller switch-group on page 1013](#)
- [config switch-controller switch-interface-tag on page 1014](#)
- [config switch-controller switch-log on page 1015](#)
- [config switch-controller switch-profile on page 1016](#)
- [config switch-controller system on page 1018](#)
- [config switch-controller traffic-policy on page 1020](#)
- [config switch-controller traffic-sniffer on page 1022](#)
- [config switch-controller virtual-port-pool on page 1024](#)
- [config switch-controller vlan-policy on page 1025](#)

## config switch-controller 802-1X-settings



This command is available for model(s): FortiGate 1000D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001E1, FortiGate 5001E.

Configure global 802.1X settings.

```
config switch-controller 802-1X-settings
    Description: Configure global 802.1X settings.
    set link-down-auth [set-unauth|no-action]
    set max-reauth-attempt {integer}
    set reauth-period {integer}
    set tx-period {integer}
end
```

## config switch-controller 802-1X-settings

Parameter	Description	Type	Size	Default						
link-down-auth	Interface-reauthentication state to set if a link is down.	option	-	set-unauth						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>set-unauth</i></td><td>Interface set to unauth when down. Reauthentication is needed.</td></tr><tr><td><i>no-action</i></td><td>Interface reauthentication is not needed.</td></tr></table>	Option	Description	<i>set-unauth</i>	Interface set to unauth when down. Reauthentication is needed.	<i>no-action</i>	Interface reauthentication is not needed.			
Option	Description									
<i>set-unauth</i>	Interface set to unauth when down. Reauthentication is needed.									
<i>no-action</i>	Interface reauthentication is not needed.									
max-reauth-attempt	Maximum number of authentication attempts.	integer	Minimum value: 0 Maximum value: 15	3						
reauth-period	Period of time to allow for reauthentication.	integer	Minimum value: 0 Maximum value: 1440	60						
tx-period	802.1X Tx period.	integer	Minimum value: 4 Maximum value: 60	30						



## config switch-controller auto-config custom



This command is available for model(s): FortiGate 1000D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001E1, FortiGate 5001E.

Policies which can override the 'default' for specific ISL/ICL/FortiLink interface.

```
config switch-controller auto-config custom
    Description: Policies which can override the 'default' for specific ISL/ICL/FortiLink
interface.
    edit <name>
        config switch-binding
            Description: Switch binding list.
            edit <switch-id>
                set policy {string}
            next
        end
    next
end
```

## config switch-controller auto-config custom

Parameter	Description	Type	Size	Default
name	Auto-Config FortiLink or ISL/ICL interface name.	string	Maximum length: 15	

## config switch-binding

Parameter	Description	Type	Size	Default
switch-id	Switch name.	string	Maximum length: 16	
policy	Custom auto-config policy.	string	Maximum length: 63	default

## config switch-controller auto-config default



This command is available for model(s): FortiGate 1000D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001E1, FortiGate 5001E.

Policies which are applied automatically to all ISL/ICL/FortiLink interfaces.

```
config switch-controller auto-config default
    Description: Policies which are applied automatically to all ISL/ICL/FortiLink
interfaces.
    set fgt-policy {string}
    set icl-policy {string}
    set isl-policy {string}
end
```

## config switch-controller auto-config default

Parameter	Description	Type	Size	Default
fgt-policy	Default FortiLink auto-config policy.	string	Maximum length: 63	default
icl-policy	Default ICL auto-config policy.	string	Maximum length: 63	default-icl
isl-policy	Default ISL auto-config policy.	string	Maximum length: 63	default

## config switch-controller auto-config policy



This command is available for model(s): FortiGate 1000D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001E1, FortiGate 5001E.

Policy definitions which can define the behavior on auto configured interfaces.

```
config switch-controller auto-config policy
```

Description: Policy definitions which can define the behavior on auto configured interfaces.

```
edit <name>
    set igmp-flood-report [enable|disable]
    set igmp-flood-traffic [enable|disable]
    set poe-status [enable|disable]
    set qos-policy {string}
    set storm-control-policy {string}
```

```
next
end
```

## config switch-controller auto-config policy

Parameter	Description	Type	Size	Default						
igmp-flood-report	Enable/disable IGMP flood report.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable IGMP flood report.</td></tr><tr><td><i>disable</i></td><td>Disable IGMP flood report.</td></tr></table>	Option	Description	<i>enable</i>	Enable IGMP flood report.	<i>disable</i>	Disable IGMP flood report.			
Option	Description									
<i>enable</i>	Enable IGMP flood report.									
<i>disable</i>	Disable IGMP flood report.									
igmp-flood-traffic	Enable/disable IGMP flood traffic.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable IGMP flood traffic.</td></tr><tr><td><i>disable</i></td><td>Disable IGMP flood traffic.</td></tr></table>	Option	Description	<i>enable</i>	Enable IGMP flood traffic.	<i>disable</i>	Disable IGMP flood traffic.			
Option	Description									
<i>enable</i>	Enable IGMP flood traffic.									
<i>disable</i>	Disable IGMP flood traffic.									
name	Auto-config policy name.	string	Maximum length: 63							
poe-status	Enable/disable PoE status.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable PoE status.</td></tr><tr><td><i>disable</i></td><td>Disable PoE status.</td></tr></table>	Option	Description	<i>enable</i>	Enable PoE status.	<i>disable</i>	Disable PoE status.			
Option	Description									
<i>enable</i>	Enable PoE status.									
<i>disable</i>	Disable PoE status.									
qos-policy	Auto-Config QoS policy.	string	Maximum length: 63	default						
storm-control-policy	Auto-Config storm control policy.	string	Maximum length: 63	auto-config						

## config switch-controller custom-command



This command is available for model(s): FortiGate 1000D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001E1, FortiGate 5001E.

Configure the FortiGate switch controller to send custom commands to managed FortiSwitch devices.

```
config switch-controller custom-command
    Description: Configure the FortiGate switch controller to send custom commands to
managed FortiSwitch devices.
    edit <command-name>
        set command {var-string}
        set description {string}
    next
end
```

## config switch-controller custom-command

Parameter	Description	Type	Size	Default
command	String of commands to send to FortiSwitch devices (For example (%0a = return key): config switch trunk %0a edit myTrunk %0a set members port1 port2 %0a end %0a).	var-string	Maximum length: 4095	
command-name	Command name called by the FortiGate switch controller in the execute command.	string	Maximum length: 35	
description	Description.	string	Maximum length: 35	

## config switch-controller dsl policy



This command is available for model(s): FortiGate 40F 3G4G, FortiGate 60F, FortiGate 80F Bypass, FortiGate 80F, FortiGate 81F, FortiGateRugged 60F 3G4G, FortiGateRugged 60F. It is not available for: FortiGate 1000D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 61E, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F-POE, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate VM64, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

DSL policy.

```
config switch-controller dsl policy
  Description: DSL policy.
  edit <name>
    set append_padding [disable|enable]
    set cpe-aele [disable|enable]
    set cpe-aele-mode [ELE_M0|ELE_DS|...]
    set cs {option1}, {option2}, ...
    set ds-bitswap [disable|enable]
    set pause-frame [disable|enable]
    set profile [auto-30a|auto-17a|...]
    set type {option}
    set us-bitswap [disable|enable]
  next
end
```

## config switch-controller dsl policy

Parameter	Description	Type	Size	Default
append_padding	device pause frame configuration.	option	-	enable

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable.		
	<i>enable</i>	Enable.		
cpe-aele	cpe AELE.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable.		
	<i>enable</i>	Enable.		
cpe-aele-mode	cpe AELE-Mode with given string.	option	-	ELE_MIN
	<b>Option</b>	<b>Description</b>		
	<i>ELE_M0</i>	cpe AELE-Mode with given string.		
	<i>ELE_DS</i>	cpe AELE-Mode with given string.		
	<i>ELE_PB</i>	cpe AELE-Mode with given string.		
	<i>ELE_MIN</i>	cpe AELE-Mode with given string.		
cs	CPE carrier set.	option	-	A43 B43 A43C
	<b>Option</b>	<b>Description</b>		
	<i>A43</i>	CPE carrier set.		
	<i>B43</i>	CPE carrier set.		
	<i>A43C</i>	CPE carrier set.		
	<i>V43</i>	CPE carrier set.		
ds-bitswap	Enable/disable bitswap.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable.		
	<i>enable</i>	Enable.		
name	Policy name.	string	Maximum length: 63	
pause-frame	device pause frame configuration.	option	-	enable

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable.		
	<i>enable</i>	Enable.		
profile	vdsl CPE profile.	option	-	auto-30a
	<b>Option</b>	<b>Description</b>		
	<i>auto-30a</i>	vdsl CPE profile.		
	<i>auto-17a</i>	vdsl CPE profile.		
	<i>auto-12ab</i>	vdsl CPE profile.		
type	Type.	option	-	Proscend
	<b>Option</b>	<b>Description</b>		
	<i>Proscend</i>	Proscend.		
us-bitswap	Enable/disable bitswap.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable.		
	<i>enable</i>	Enable.		



## config switch-controller dynamic-port-policy



This command is available for model(s): FortiGate 1000D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001E1, FortiGate 5001E.

Configure Dynamic port policy to be applied on the managed FortiSwitch ports through DPP device.

```
config switch-controller dynamic-port-policy
```

Description: Configure Dynamic port policy to be applied on the managed FortiSwitch ports through DPP device.

```
edit <name>
    set description {string}
    set fortilink {string}
    config policy
        Description: Port policies with matching criteria and actions.
        edit <name>
            set description {string}
            set status [enable|disable]
            set category [device|interface-tag]
            set interface-tags <tag-name1>, <tag-name2>, ...
            set mac {string}
            set hw-vendor {string}
            set type {string}
            set family {string}
            set host {string}
            set lldp-profile {string}
            set qos-policy {string}
            set 802-1x {string}
            set vlan-policy {string}
            set bounce-port-link [disable|enable]
        next
    end
```

```
next
end
```

## config switch-controller dynamic-port-policy

Parameter	Description	Type	Size	Default
description	Description for the Dynamic port policy.	string	Maximum length: 63	
fortilink	FortiLink interface for which this Dynamic port policy belongs to.	string	Maximum length: 15	
name	Dynamic port policy name.	string	Maximum length: 63	

## config policy

Parameter	Description	Type	Size	Default						
name	Policy name.	string	Maximum length: 63							
description	Description for the policy.	string	Maximum length: 63							
status	Enable/disable policy.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable policy.</td></tr><tr><td><i>disable</i></td><td>Disable policy.</td></tr></table>				Option	Description	<i>enable</i>	Enable policy.	<i>disable</i>	Disable policy.
	Option	Description								
	<i>enable</i>	Enable policy.								
<i>disable</i>	Disable policy.									
category	Category of Dynamic port policy.	option	-	device						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>device</i></td><td>Device category.</td></tr><tr><td><i>interface-tag</i></td><td>Interface Tag category.</td></tr></table>				Option	Description	<i>device</i>	Device category.	<i>interface-tag</i>	Interface Tag category.
	Option	Description								
	<i>device</i>	Device category.								
<i>interface-tag</i>	Interface Tag category.									
interface-tags <tag-name>	Match policy based on the FortiSwitch interface object tags. FortiSwitch port tag name.	string	Maximum length: 63							
mac	Match policy based on MAC address.	string	Maximum length: 17							
hw-vendor	Match policy based on hardware vendor.	string	Maximum length: 15							
type	Match policy based on type.	string	Maximum length: 15							

Parameter	Description	Type	Size	Default
family	Match policy based on family.	string	Maximum length: 31	
host	Match policy based on host.	string	Maximum length: 64	
lldp-profile	LLDP profile to be applied when using this policy.	string	Maximum length: 63	
qos-policy	QoS policy to be applied when using this policy.	string	Maximum length: 63	
802-1x	802.1x security policy to be applied when using this policy.	string	Maximum length: 31	
vlan-policy	VLAN policy to be applied when using this policy.	string	Maximum length: 63	
bounce-port-link	Enable/disable bouncing (administratively bring the link down, up) of a switch port where this policy is applied. Helps to clear and reassign VLAN from lldp-profile.	option	-	enable
		Option	Description	
		<i>disable</i>	Disable bouncing (administratively bring the link down, up) of a switch port where this policy is applied.	
		<i>enable</i>	Enable bouncing (administratively bring the link down, up) of a switch port where this policy is applied.	

---

## config switch-controller flow-tracking

---



This command is available for model(s): FortiGate 1000D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001E1, FortiGate 5001E.

---

### Configure FortiSwitch flow tracking and export via ipfix/netflow.

```
config switch-controller flow-tracking
    Description: Configure FortiSwitch flow tracking and export via ipfix/netflow.
    config aggregates
        Description: Configure aggregates in which all traffic sessions matching the IP
        Address will be grouped into the same flow.
        edit <id>
            set ip {ipv4-classnet}
            next
        end
        set collector-ip {ipv4-address}
        set collector-port {integer}
        set format [netflow1|netflow5|...]
        set level [vlan|ip|...]
        set max-export-pkt-size {integer}
        set sample-mode [local|perimeter|...]
        set sample-rate {integer}
        set timeout-general {integer}
        set timeout-icmp {integer}
        set timeout-max {integer}
        set timeout-tcp {integer}
        set timeout-tcp-fin {integer}
        set timeout-tcp-rst {integer}
        set timeout-udp {integer}
        set transport [udp|tcp|...]
    end
```

## config switch-controller flow-tracking

Parameter	Description	Type	Size	Default												
collector-ip	Configure collector ip address.	ipv4-address	Not Specified	0.0.0.0												
collector-port	Configure collector port number.	integer	Minimum value: 0 Maximum value: 65535	0												
format	Configure flow tracking protocol.	option	-	netflow9												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>netflow1</td><td>Netflow version 1 sampling.</td></tr><tr><td>netflow5</td><td>Netflow version 5 sampling.</td></tr><tr><td>netflow9</td><td>Netflow version 9 sampling.</td></tr><tr><td>ipfix</td><td>Ipfix sampling.</td></tr></table>				Option	Description	netflow1	Netflow version 1 sampling.	netflow5	Netflow version 5 sampling.	netflow9	Netflow version 9 sampling.	ipfix	Ipfix sampling.		
Option	Description															
netflow1	Netflow version 1 sampling.															
netflow5	Netflow version 5 sampling.															
netflow9	Netflow version 9 sampling.															
ipfix	Ipfix sampling.															
level	Configure flow tracking level.	option	-	ip												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>vlan</td><td>Collects srcip/dstip/srcport/dstport/protocol/tos/vlan from the sample packet.</td></tr><tr><td>ip</td><td>Collects srcip/dstip from the sample packet.</td></tr><tr><td>port</td><td>Collects srcip/dstip/srcport/dstport/protocol from the sample packet.</td></tr><tr><td>proto</td><td>Collects srcip/dstip/protocol from the sample packet.</td></tr><tr><td>mac</td><td>Collects smac/dmac from the sample packet.</td></tr></table>				Option	Description	vlan	Collects srcip/dstip/srcport/dstport/protocol/tos/vlan from the sample packet.	ip	Collects srcip/dstip from the sample packet.	port	Collects srcip/dstip/srcport/dstport/protocol from the sample packet.	proto	Collects srcip/dstip/protocol from the sample packet.	mac	Collects smac/dmac from the sample packet.
Option	Description															
vlan	Collects srcip/dstip/srcport/dstport/protocol/tos/vlan from the sample packet.															
ip	Collects srcip/dstip from the sample packet.															
port	Collects srcip/dstip/srcport/dstport/protocol from the sample packet.															
proto	Collects srcip/dstip/protocol from the sample packet.															
mac	Collects smac/dmac from the sample packet.															
max-export-pkt-size	Configure flow max export packet size.	integer	Minimum value: 512 Maximum value: 9216	512												
sample-mode	Configure sample mode for the flow tracking.	option	-	perimeter												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>local</td><td>Set local mode which samples on the specific switch port.</td></tr><tr><td>perimeter</td><td>Set perimeter mode which samples on all switch fabric ports and fortilink port at the ingress.</td></tr><tr><td>device-ingress</td><td>Set device -ingress mode which samples across all switch ports at the ingress.</td></tr></table>				Option	Description	local	Set local mode which samples on the specific switch port.	perimeter	Set perimeter mode which samples on all switch fabric ports and fortilink port at the ingress.	device-ingress	Set device -ingress mode which samples across all switch ports at the ingress.				
Option	Description															
local	Set local mode which samples on the specific switch port.															
perimeter	Set perimeter mode which samples on all switch fabric ports and fortilink port at the ingress.															
device-ingress	Set device -ingress mode which samples across all switch ports at the ingress.															
sample-rate	Configure sample rate for the perimeter and device-ingress sampling.	integer	Minimum value: 0 Maximum value: 99999	512												

Parameter	Description	Type	Size	Default
timeout-general	Configure flow session general timeout.	integer	Minimum value: 3600 60 Maximum value: 604800	3600
timeout-icmp	Configure flow session ICMP timeout.	integer	Minimum value: 300 60 Maximum value: 604800	300
timeout-max	Configure flow session max timeout.	integer	Minimum value: 604800 60 Maximum value: 604800	604800
timeout-tcp	Configure flow session TCP timeout.	integer	Minimum value: 3600 60 Maximum value: 604800	3600
timeout-tcp-fin	Configure flow session TCP FIN timeout.	integer	Minimum value: 300 60 Maximum value: 604800	300
timeout-tcp-rst	Configure flow session TCP RST timeout.	integer	Minimum value: 120 60 Maximum value: 604800	120
timeout-udp	Configure flow session UDP timeout.	integer	Minimum value: 300 60 Maximum value: 604800	300
transport	Configure L4 transport protocol for exporting packets.	option	-	udp

Option	Description
<i>udp</i>	UDP protocol.
<i>tcp</i>	TCP protocol.
<i>sctp</i>	SCTP protocol.

## config aggregates

Parameter	Description	Type	Size	Default
id	Aggregate id.	integer	Minimum value: 0 Maximum value: 4294967295	0
ip	IP address to group all matching traffic sessions to a flow.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0

---

## config switch-controller fortilink-settings

---



This command is available for model(s): FortiGate 1000D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001E1, FortiGate 5001E.

---

Configure integrated FortiLink settings for FortiSwitch.

```
config switch-controller fortilink-settings
  Description: Configure integrated FortiLink settings for FortiSwitch.
  edit <name>
    set fortilink {string}
    set inactive-timer {integer}
    set link-down-flush [disable|enable]
    config nac-ports
      Description: NAC specific configuration.
      set onboarding-vlan {string}
      set lan-segment [enabled|disabled]
      set nac-lan-interface {string}
      set nac-segment-vlans <vlan-name1>, <vlan-name2>, ...
      set parent-key {string}
      set member-change {integer}
    end
  next
end
```

## config switch-controller fortilink-settings

Parameter	Description	Type	Size	Default						
fortilink	FortiLink interface to which this fortilink-setting belongs.	string	Maximum length: 15							
inactive-timer	Time interval(minutes) to be included in the inactive devices expiry calculation (mac age-out + inactive-time + periodic scan interval).	integer	Minimum value: 1 Maximum value: 1440	15						
link-down-flush	Clear NAC and dynamic devices on switch ports on link down event.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable clearing NAC and dynamic devices on a switch port when link down event happens.</td></tr><tr><td><i>enable</i></td><td>Enable clearing NAC and dynamic devices on a switch port when link down event happens.</td></tr></table>				Option	Description	<i>disable</i>	Disable clearing NAC and dynamic devices on a switch port when link down event happens.	<i>enable</i>	Enable clearing NAC and dynamic devices on a switch port when link down event happens.
Option	Description									
<i>disable</i>	Disable clearing NAC and dynamic devices on a switch port when link down event happens.									
<i>enable</i>	Enable clearing NAC and dynamic devices on a switch port when link down event happens.									
name	FortiLink settings name.	string	Maximum length: 35							

## config nac-ports

Parameter	Description	Type	Size	Default
onboarding-vlan	Default NAC Onboarding VLAN when NAC devices are discovered.	string	Maximum length: 15	
lan-segment	Enable/disable LAN segment feature on the FortiLink interface.	option	-	disabled
	Option	Description		
	enabled	Enable lan-segment on this interface.		
	disabled	Disable lan-segment on this interface.		
nac-lan-interface	Configure NAC LAN interface.	string	Maximum length: 15	
nac-segment-vlans <vlan-name>	Configure NAC segment VLANs. VLAN interface name.	string	Maximum length: 79	
parent-key	Parent key name.	string	Maximum length: 35	



Parameter	Description	Type	Size	Default
member-change	Member change flag.	integer	Minimum value: 0 Maximum value: 255	0

## config switch-controller global



This command is available for model(s): FortiGate 1000D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001E1, FortiGate 5001E.

Configure FortiSwitch global settings.

```
config switch-controller global
    Description: Configure FortiSwitch global settings.
    set bounce-quarantined-link [disable|enable]
    config custom-command
        Description: List of custom commands to be pushed to all FortiSwitches in the VDOM.
        edit <command-entry>
            set command-name {string}
        next
    end
    set default-virtual-switch-vlan {string}
    set dhcp-server-access-list [enable|disable]
    set disable-discovery <name1>, <name2>, ...
    set fips-enforce [disable|enable]
    set firmware-provision-on-authorization [enable|disable]
    set https-image-push [enable|disable]
    set log-mac-limit-violations [enable|disable]
```

```

set mac-aging-interval {integer}
set mac-event-logging [enable|disable]
set mac-retention-period {integer}
set mac-violation-timer {integer}
set quarantine-mode [by-vlan|by-redirect]
set sn-dns-resolution [enable|disable]
set update-user-device {option1}, {option2}, ...
set vlan-all-mode [all|defined]
set vlan-optimization [enable|disable]

```

end

## config switch-controller global

Parameter	Description	Type	Size	Default						
bounce-quarantined-link	Enable/disable bouncing (administratively bring the link down, up) of a switch port where a quarantined device was seen last. Helps to re-initiate the DHCP process for a device.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable bouncing (administratively bring the link down, up) of a switch port where a quarantined device was seen last.</td></tr><tr><td>enable</td><td>Enable bouncing (administratively bring the link down, up) of a switch port where a quarantined device was seen last.</td></tr></table>				Option	Description	disable	Disable bouncing (administratively bring the link down, up) of a switch port where a quarantined device was seen last.	enable	Enable bouncing (administratively bring the link down, up) of a switch port where a quarantined device was seen last.
Option	Description									
disable	Disable bouncing (administratively bring the link down, up) of a switch port where a quarantined device was seen last.									
enable	Enable bouncing (administratively bring the link down, up) of a switch port where a quarantined device was seen last.									
default-virtual-switch-vlan	Default VLAN for ports when added to the virtual-switch.	string	Maximum length: 15							
dhcp-server-access-list	Enable/disable DHCP snooping server access list.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable DHCP server access list.</td></tr><tr><td>disable</td><td>Disable DHCP server access list.</td></tr></table>				Option	Description	enable	Enable DHCP server access list.	disable	Disable DHCP server access list.
Option	Description									
enable	Enable DHCP server access list.									
disable	Disable DHCP server access list.									
disable-discovery<name>	Prevent this FortiSwitch from discovering. Managed device ID.	string	Maximum length: 79							
fips-enforce	Enable/disable enforcement of FIPS on managed FortiSwitch devices.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable enforcement of FIPS on managed FortiSwitch devices.</td></tr><tr><td>enable</td><td>Enable enforcement of FIPS on managed FortiSwitch devices.</td></tr></table>				Option	Description	disable	Disable enforcement of FIPS on managed FortiSwitch devices.	enable	Enable enforcement of FIPS on managed FortiSwitch devices.
Option	Description									
disable	Disable enforcement of FIPS on managed FortiSwitch devices.									
enable	Enable enforcement of FIPS on managed FortiSwitch devices.									

Parameter	Description	Type	Size	Default						
firmware-provision-on-authorization	Enable/disable automatic provisioning of latest firmware on authorization.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable firmware provision on authorization.</td></tr><tr><td><i>disable</i></td><td>Disable firmware provision on authorization.</td></tr></table>	Option	Description	<i>enable</i>	Enable firmware provision on authorization.	<i>disable</i>	Disable firmware provision on authorization.			
Option	Description									
<i>enable</i>	Enable firmware provision on authorization.									
<i>disable</i>	Disable firmware provision on authorization.									
https-image-push	Enable/disable image push to FortiSwitch using HTTPS.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable image push to FortiSwitch using HTTPS.</td></tr><tr><td><i>disable</i></td><td>Disable image push to FortiSwitch using HTTPS.</td></tr></table>	Option	Description	<i>enable</i>	Enable image push to FortiSwitch using HTTPS.	<i>disable</i>	Disable image push to FortiSwitch using HTTPS.			
Option	Description									
<i>enable</i>	Enable image push to FortiSwitch using HTTPS.									
<i>disable</i>	Disable image push to FortiSwitch using HTTPS.									
log-mac-limit-violations	Enable/disable logs for Learning Limit Violations.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Learn Limit Violation.</td></tr><tr><td><i>disable</i></td><td>Disable Learn Limit Violation.</td></tr></table>	Option	Description	<i>enable</i>	Enable Learn Limit Violation.	<i>disable</i>	Disable Learn Limit Violation.			
Option	Description									
<i>enable</i>	Enable Learn Limit Violation.									
<i>disable</i>	Disable Learn Limit Violation.									
mac-aging-interval	Time after which an inactive MAC is aged out.	integer	Minimum value: 10 Maximum value: 1000000	300						
mac-event-logging	Enable/disable MAC address event logging.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable MAC address event logging.</td></tr><tr><td><i>disable</i></td><td>Disable MAC address event logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable MAC address event logging.	<i>disable</i>	Disable MAC address event logging.			
Option	Description									
<i>enable</i>	Enable MAC address event logging.									
<i>disable</i>	Disable MAC address event logging.									
mac-retention-period	Time in hours after which an inactive MAC is removed from client DB (0 = aged out based on mac-aging-interval).	integer	Minimum value: 0 Maximum value: 168	24						

Parameter	Description	Type	Size	Default												
mac-violation-timer	Set timeout for Learning Limit Violations (0 = disabled).	integer	Minimum value: 0 Maximum value: 4294967295	0												
quarantine-mode	Quarantine mode.	option	-	by-vlan												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>by-vlan</td><td>Quarantined device traffic is sent to FortiGate on a separate quarantine VLAN.</td></tr><tr><td>by-redirect</td><td>Quarantined device traffic is redirected only to the FortiGate on the received VLAN.</td></tr></table>	Option	Description	by-vlan	Quarantined device traffic is sent to FortiGate on a separate quarantine VLAN.	by-redirect	Quarantined device traffic is redirected only to the FortiGate on the received VLAN.									
Option	Description															
by-vlan	Quarantined device traffic is sent to FortiGate on a separate quarantine VLAN.															
by-redirect	Quarantined device traffic is redirected only to the FortiGate on the received VLAN.															
sn-dns-resolution	Enable/disable DNS resolution of the FortiSwitch unit's IP address by use of its serial number.	option	-	enable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable DNS resolution of the FortiSwitch unit's IP address by use of its serial number.</td></tr><tr><td>disable</td><td>Disable DNS resolution of the FortiSwitch unit's IP address by use of its serial number.</td></tr></table>	Option	Description	enable	Enable DNS resolution of the FortiSwitch unit's IP address by use of its serial number.	disable	Disable DNS resolution of the FortiSwitch unit's IP address by use of its serial number.									
Option	Description															
enable	Enable DNS resolution of the FortiSwitch unit's IP address by use of its serial number.															
disable	Disable DNS resolution of the FortiSwitch unit's IP address by use of its serial number.															
update-user-device	Control which sources update the device user list.	option	-	mac-cache lldp dhcp-snooping l2-db l3-db												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>mac-cache</td><td>Update MAC address from switch-controller mac-cache.</td></tr><tr><td>lldp</td><td>Update from FortiSwitch LLDP neighbor database.</td></tr><tr><td>dhcp-snooping</td><td>Update from FortiSwitch DHCP snooping client and server databases.</td></tr><tr><td>l2-db</td><td>Update from FortiSwitch Network-monitor Layer 2 tracking database.</td></tr><tr><td>l3-db</td><td>Update from FortiSwitch Network-monitor Layer 3 tracking database.</td></tr></table>	Option	Description	mac-cache	Update MAC address from switch-controller mac-cache.	lldp	Update from FortiSwitch LLDP neighbor database.	dhcp-snooping	Update from FortiSwitch DHCP snooping client and server databases.	l2-db	Update from FortiSwitch Network-monitor Layer 2 tracking database.	l3-db	Update from FortiSwitch Network-monitor Layer 3 tracking database.			
Option	Description															
mac-cache	Update MAC address from switch-controller mac-cache.															
lldp	Update from FortiSwitch LLDP neighbor database.															
dhcp-snooping	Update from FortiSwitch DHCP snooping client and server databases.															
l2-db	Update from FortiSwitch Network-monitor Layer 2 tracking database.															
l3-db	Update from FortiSwitch Network-monitor Layer 3 tracking database.															
vlan-all-mode	VLAN configuration mode, user-defined-vlans or all-possible-vlans.	option	-	defined												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>all</td><td>Include all possible VLANs (1-4093).</td></tr><tr><td>defined</td><td>Include user defined VLANs.</td></tr></table>	Option	Description	all	Include all possible VLANs (1-4093).	defined	Include user defined VLANs.									
Option	Description															
all	Include all possible VLANs (1-4093).															
defined	Include user defined VLANs.															

Parameter	Description	Type	Size	Default
vlan-optimization	FortiLink VLAN optimization.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable VLAN optimization on FortiSwitch units for auto-generated trunks.		
	<i>disable</i>	Disable VLAN optimization on FortiSwitch units for auto-generated trunks.		

## config custom-command

Parameter	Description	Type	Size	Default
command-entry	List of FortiSwitch commands.	string	Maximum length: 35	
command-name	Name of custom command to push to all FortiSwitches in VDOM.	string	Maximum length: 35	

## config switch-controller igmp-snooping



This command is available for model(s): FortiGate 1000D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001E1, FortiGate 5001E.

Configure FortiSwitch IGMP snooping global settings.

```

config switch-controller igmp-snooping
    Description: Configure FortiSwitch IGMP snooping global settings.
    set aging-time {integer}
    set flood-unknown-multicast [enable|disable]
    set query-interval {integer}
end

```

## config switch-controller igmp-snooping

Parameter	Description	Type	Size	Default						
aging-time	Maximum number of seconds to retain a multicast snooping entry for which no packets have been seen.	integer	Minimum value: 15 Maximum value: 3600	300						
flood-unknown-multicast	Enable/disable unknown multicast flooding.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable unknown multicast flooding.</td></tr><tr><td><i>disable</i></td><td>Disable unknown multicast flooding.</td></tr></table>				Option	Description	<i>enable</i>	Enable unknown multicast flooding.	<i>disable</i>	Disable unknown multicast flooding.
	Option	Description								
	<i>enable</i>	Enable unknown multicast flooding.								
<i>disable</i>	Disable unknown multicast flooding.									
query-interval	Maximum time after which IGMP query will be sent.	integer	Minimum value: 10 Maximum value: 1200	125						

## config switch-controller initial-config template



This command is available for model(s): FortiGate 1000D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3900E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001E1, FortiGate 5001E.

Configure template for auto-generated VLANs.

```
config switch-controller initial-config template
  Description: Configure template for auto-generated VLANs.
  edit <name>
    set allowaccess {option1}, {option2}, ...
    set auto-ip [enable|disable]
    set dhcp-server [enable|disable]
    set ip {ipv4-classnet-host}
    set vlanid {integer}
  next
end
```

## config switch-controller initial-config template

Parameter	Description	Type	Size	Default				
allowaccess	Permitted types of management access to this interface.	option	-					
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ping</i></td><td>PING access.</td></tr></table>	Option	Description	<i>ping</i>	PING access.			
Option	Description							
<i>ping</i>	PING access.							

Parameter	Description	Type	Size	Default																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>https</i></td><td>HTTPS access.</td></tr><tr><td><i>ssh</i></td><td>SSH access.</td></tr><tr><td><i>snmp</i></td><td>SNMP access.</td></tr><tr><td><i>http</i></td><td>HTTP access.</td></tr><tr><td><i>telnet</i></td><td>TELNET access.</td></tr><tr><td><i>fgfm</i></td><td>FortiManager access.</td></tr><tr><td><i>radius-acct</i></td><td>RADIUS accounting access.</td></tr><tr><td><i>probe-response</i></td><td>Probe access.</td></tr><tr><td><i>fabric</i></td><td>Security Fabric access.</td></tr><tr><td><i>ftm</i></td><td>FTM access.</td></tr></table>	Option	Description	<i>https</i>	HTTPS access.	<i>ssh</i>	SSH access.	<i>snmp</i>	SNMP access.	<i>http</i>	HTTP access.	<i>telnet</i>	TELNET access.	<i>fgfm</i>	FortiManager access.	<i>radius-acct</i>	RADIUS accounting access.	<i>probe-response</i>	Probe access.	<i>fabric</i>	Security Fabric access.	<i>ftm</i>	FTM access.			
	Option	Description																								
	<i>https</i>	HTTPS access.																								
	<i>ssh</i>	SSH access.																								
	<i>snmp</i>	SNMP access.																								
	<i>http</i>	HTTP access.																								
	<i>telnet</i>	TELNET access.																								
	<i>fgfm</i>	FortiManager access.																								
	<i>radius-acct</i>	RADIUS accounting access.																								
	<i>probe-response</i>	Probe access.																								
	<i>fabric</i>	Security Fabric access.																								
<i>ftm</i>	FTM access.																									
auto-ip	Automatically allocate interface address and subnet block.	option	-	enable																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable auto-ip status.</td></tr><tr><td><i>disable</i></td><td>Disable auto-ip status.</td></tr></table>	Option	Description	<i>enable</i>	Enable auto-ip status.	<i>disable</i>	Disable auto-ip status.																			
	Option	Description																								
	<i>enable</i>	Enable auto-ip status.																								
<i>disable</i>	Disable auto-ip status.																									
dhcp-server	Enable/disable a DHCP server on this interface.	option	-	disable																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable DHCP server.</td></tr><tr><td><i>disable</i></td><td>Disable DHCP server.</td></tr></table>	Option	Description	<i>enable</i>	Enable DHCP server.	<i>disable</i>	Disable DHCP server.																			
	Option	Description																								
	<i>enable</i>	Enable DHCP server.																								
<i>disable</i>	Disable DHCP server.																									
ip	Interface IPv4 address and subnet mask.	ipv4-classnet-host	Not Specified	0.0.0.0 0.0.0.0																						
name	Initial config template name.	string	Maximum length: 63																							
vlanid	Unique VLAN ID.	integer	Minimum value: 1 Maximum value: 4094	0																						



## config switch-controller initial-config vlans



This command is available for model(s): FortiGate 1000D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001E1, FortiGate 5001E.

Configure initial template for auto-generated VLAN interfaces.

```
config switch-controller initial-config vlans
    Description: Configure initial template for auto-generated VLAN interfaces.
    set default-vlan {string}
    set nac {string}
    set nac-segment {string}
    set quarantine {string}
    set rspan {string}
    set video {string}
    set voice {string}
end
```

## config switch-controller initial-config vlans

Parameter	Description	Type	Size	Default
default-vlan	Default VLAN (native) assigned to all switch ports upon discovery.	string	Maximum length: 63	_default
nac	VLAN for NAC onboarding devices.	string	Maximum length: 63	onboarding
nac-segment	VLAN for NAC segment primary interface.	string	Maximum length: 63	nac_segment

Parameter	Description	Type	Size	Default
quarantine	VLAN for quarantined traffic.	string	Maximum length: 63	quarantine
rspan	VLAN for RSPAN/ERSPAN mirrored traffic.	string	Maximum length: 63	rspan
video	VLAN dedicated for video devices.	string	Maximum length: 63	video
voice	VLAN dedicated for voice devices.	string	Maximum length: 63	voice

## config switch-controller lldp-profile



This command is available for model(s): FortiGate 1000D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001E1, FortiGate 5001E.

Configure FortiSwitch LLDP profiles.

```
config switch-controller lldp-profile
  Description: Configure FortiSwitch LLDP profiles.
  edit <name>
    set 802 1-tlvs {option1}, {option2}, ...
    set 802 3-tlvs {option1}, {option2}, ...
    set auto-isl [disable|enable]
    set auto-isl-hello-timer {integer}
    set auto-isl-port-group {integer}
    set auto-isl-receive-timeout {integer}
    set auto-mclag-icl [disable|enable]
```

```

config custom-tlvs
    Description: Configuration method to edit custom TLV entries.
    edit <name>
        set oui {user}
        set subtype {integer}
        set information-string {user}
    next
end
config med-location-service
    Description: Configuration method to edit Media Endpoint Discovery (MED)
location service type-length-value (TLV) categories.
    edit <name>
        set status [disable|enable]
        set sys-location-id {string}
    next
end
config med-network-policy
    Description: Configuration method to edit Media Endpoint Discovery (MED) network
policy type-length-value (TLV) categories.
    edit <name>
        set status [disable|enable]
        set vlan-intf {string}
        set assign-vlan [disable|enable]
        set priority {integer}
        set dscp {integer}
    next
end
set med-tlvs {option1}, {option2}, ...
next
end

```

## config switch-controller lldp-profile

Parameter	Description	Type	Size	Default						
802 1-tlvs	Transmitted IEEE 802.1 TLVs.	option	-							
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>port-vlan-id</i></td><td>Port native VLAN TLV.</td></tr></table>	Option	Description	<i>port-vlan-id</i>	Port native VLAN TLV.					
Option	Description									
<i>port-vlan-id</i>	Port native VLAN TLV.									
802 3-tlvs	Transmitted IEEE 802.3 TLVs.	option	-							
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>max-frame-size</i></td><td>Maximum frame size TLV.</td></tr><tr><td><i>power-negotiation</i></td><td>PoE+ classification TLV.</td></tr></table>	Option	Description	<i>max-frame-size</i>	Maximum frame size TLV.	<i>power-negotiation</i>	PoE+ classification TLV.			
Option	Description									
<i>max-frame-size</i>	Maximum frame size TLV.									
<i>power-negotiation</i>	PoE+ classification TLV.									
auto-isf	Enable/disable auto inter-switch LAG.	option	-	enable						

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable automatic MCLAG inter chassis link.		
	<i>enable</i>	Enable automatic MCLAG inter chassis link.		
auto-isl-hello-timer	Auto inter-switch LAG hello timer duration.	integer	Minimum value: 1 Maximum value: 30	3
auto-isl-port-group	Auto inter-switch LAG port group ID.	integer	Minimum value: 0 Maximum value: 9	0
auto-isl-receive-timeout	Auto inter-switch LAG timeout if no response is received.	integer	Minimum value: 0 Maximum value: 90	60
auto-mclag-icl	Enable/disable MCLAG inter chassis link.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable auto inter-switch-LAG.		
	<i>enable</i>	Enable auto inter-switch-LAG.		
med-tlvs	Transmitted LLDP-MED TLVs (type-length-value descriptions).	option	-	
	<b>Option</b>	<b>Description</b>		
	<i>inventory-management</i>	Inventory management TLVs.		
	<i>network-policy</i>	Network policy TLVs.		
	<i>power-management</i>	Power manangement TLVs.		
	<i>location-identification</i>	Location identificaion TLVs.		
name	Profile name.	string	Maximum length: 63	

## config custom-tlvs

Parameter	Description	Type	Size	Default
name	TLV name (not sent).	string	Maximum length: 63	
oui	Organizationally unique identifier (OUI), a 3-byte hexadecimal number, for this TLV.	user	Not Specified	000000
subtype	Organizationally defined subtype.	integer	Minimum value: 0 Maximum value: 255	0
information-string	Organizationally defined information string.	user	Not Specified	

## config med-location-service

Parameter	Description	Type	Size	Default
name	Location service type name.	string	Maximum length: 63	
status	Enable or disable this TLV.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Do not transmit this location service TLV.		
	<i>enable</i>	Transmit this location service TLV.		
sys-location-id	Location service ID.	string	Maximum length: 63	

## config med-network-policy

Parameter	Description	Type	Size	Default						
name	Policy type name.	string	Maximum length: 63							
status	Enable or disable this TLV.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Do not transmit this network policy TLV.</td></tr><tr><td><i>enable</i></td><td>Transmit this TLV if a VLAN has been added to the port.</td></tr></table>				Option	Description	<i>disable</i>	Do not transmit this network policy TLV.	<i>enable</i>	Transmit this TLV if a VLAN has been added to the port.
	Option	Description								
	<i>disable</i>	Do not transmit this network policy TLV.								
<i>enable</i>	Transmit this TLV if a VLAN has been added to the port.									
vlan-intf	VLAN interface to advertise; if configured on port.	string	Maximum length: 15							

Parameter	Description	Type	Size	Default
assign-vlan	Enable/disable VLAN assignment when this profile is applied on managed FortiSwitch port.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable VLAN assignment when this profile is applied on port.		
	<i>enable</i>	Enable VLAN assignment when this profile is applied on port.		
priority	Advertised Layer 2 priority.	integer	Minimum value: 0 Maximum value: 7	0
dscp	Advertised Differentiated Services Code Point (DSCP) value, a packet header value indicating the level of service requested for traffic, such as high priority or best effort delivery.	integer	Minimum value: 0 Maximum value: 63	0

## config switch-controller lldp-settings



This command is available for model(s): FortiGate 1000D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001E1, FortiGate 5001E.

Configure FortiSwitch LLDP settings.

```
config switch-controller lldp-settings
    Description: Configure FortiSwitch LLDP settings.
```

```

set device-detection [disable|enable]
set fast-start-interval {integer}
set management-interface [internal|mgmt]
set tx-hold {integer}
set tx-interval {integer}

```

end

## config switch-controller lldp-settings

Parameter	Description	Type	Size	Default
device-detection	Enable/disable dynamic detection of LLDP neighbor devices for VLAN assignment.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable dynamic detection of LLDP neighbor devices.		
	<i>enable</i>	Enable dynamic detection of LLDP neighbor devices.		
fast-start-interval	Frequency of LLDP PDU transmission from FortiSwitch for the first 4 packets when the link is up.	integer	Minimum value: 0 Maximum value: 255	2
management-interface	Primary management interface to be advertised in LLDP and CDP PDUs.	option	-	internal
	<b>Option</b>	<b>Description</b>		
	<i>internal</i>	Use internal interface.		
	<i>mgmt</i>	Use management interface.		
tx-hold	Number of tx-intervals before local LLDP data expires. Packet TTL is tx-hold * tx-interval.	integer	Minimum value: 1 Maximum value: 16	4
tx-interval	Frequency of LLDP PDU transmission from FortiSwitch. Packet TTL is tx-hold * tx-interval.	integer	Minimum value: 5 Maximum value: 4095	30

---

## config switch-controller location

---



This command is available for model(s): FortiGate 1000D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001E1, FortiGate 5001E.

---

### Configure FortiSwitch location services.

```
config switch-controller location
  Description: Configure FortiSwitch location services.
  edit <name>
    config address-civic
      Description: Configure location civic address.
      set additional {string}
      set additional-code {string}
      set block {string}
      set branch-road {string}
      set building {string}
      set city {string}
      set city-division {string}
      set country {string}
      set country-subdivision {string}
      set county {string}
      set direction {string}
      set floor {string}
      set landmark {string}
      set language {string}
      set name {string}
      set number {string}
      set number-suffix {string}
      set place-type {string}
      set post-office-box {string}
      set postal-community {string}
```



```

        set primary-road {string}
        set road-section {string}
        set room {string}
        set script {string}
        set seat {string}
        set street {string}
        set street-name-post-mod {string}
        set street-name-pre-mod {string}
        set street-suffix {string}
        set sub-branch-road {string}
        set trailing-str-suffix {string}
        set unit {string}
        set zip {string}
        set parent-key {string}
    end
    config coordinates
        Description: Configure location GPS coordinates.
        set altitude {string}
        set altitude-unit [m|f]
        set datum [WGS84|NAD83|...]
        set latitude {string}
        set longitude {string}
        set parent-key {string}
    end
    config elin-number
        Description: Configure location ELIN number.
        set elin-num {string}
        set parent-key {string}
    end
end
next
end

```

## config switch-controller location

Parameter	Description	Type	Size	Default
name	Unique location item name.	string	Maximum length: 63	

## config address-civic

Parameter	Description	Type	Size	Default
additional	Location additional details.	string	Maximum length: 47	
additional-code	Location additional code details.	string	Maximum length: 47	
block	Location block details.	string	Maximum length: 47	

Parameter	Description	Type	Size	Default
branch-road	Location branch road details.	string	Maximum length: 47	
building	Location building details.	string	Maximum length: 47	
city	Location city details.	string	Maximum length: 47	
city-division	Location city division details.	string	Maximum length: 47	
country	The two-letter ISO 3166 country code in capital ASCII letters eg. US, CA, DK, DE.	string	Maximum length: 47	
country-subdivision	National subdivisions (state, canton, region, province, or prefecture).	string	Maximum length: 47	
county	County, parish, gun (JP), or district (IN).	string	Maximum length: 47	
direction	Leading street direction.	string	Maximum length: 47	
floor	Floor.	string	Maximum length: 47	
landmark	Landmark or vanity address.	string	Maximum length: 47	
language	Language.	string	Maximum length: 47	
name	Name (residence and office occupant).	string	Maximum length: 47	
number	House number.	string	Maximum length: 47	
number-suffix	House number suffix.	string	Maximum length: 47	
place-type	Place type.	string	Maximum length: 47	
post-office-box	Post office box.	string	Maximum length: 47	
postal-community	Postal community name.	string	Maximum length: 47	
primary-road	Primary road name.	string	Maximum length: 47	

Parameter	Description	Type	Size	Default
road-section	Road section.	string	Maximum length: 47	
room	Room number.	string	Maximum length: 47	
script	Script used to present the address information.	string	Maximum length: 47	
seat	Seat number.	string	Maximum length: 47	
street	Street.	string	Maximum length: 47	
street-name-post-mod	Street name post modifier.	string	Maximum length: 47	
street-name-pre-mod	Street name pre modifier.	string	Maximum length: 47	
street-suffix	Street suffix.	string	Maximum length: 47	
sub-branch-road	Sub branch road name.	string	Maximum length: 47	
trailing-str-suffix	Trailing street suffix.	string	Maximum length: 47	
unit	Unit (apartment, suite).	string	Maximum length: 47	
zip	Postal/zip code.	string	Maximum length: 47	
parent-key	Parent key name.	string	Maximum length: 63	

### config coordinates

Parameter	Description	Type	Size	Default						
altitude	Plus or minus floating point number. For example, 117.47.	string	Maximum length: 15							
altitude-unit	Configure the unit for which the altitude is to (m = meters, f = floors of a building).	option	-	m						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>m</i></td><td>set altitude unit meters</td></tr><tr><td><i>f</i></td><td>set altitude unit floors</td></tr></table>				Option	Description	<i>m</i>	set altitude unit meters	<i>f</i>	set altitude unit floors
Option	Description									
<i>m</i>	set altitude unit meters									
<i>f</i>	set altitude unit floors									

Parameter	Description	Type	Size	Default
datum	WGS84, NAD83, NAD83/MLLW.	option	-	WGS84
	Option	Description		
	WGS84	set coordinates datum WGS84		
	NAD83	set coordinates datum NAD83		
	NAD83/MLLW	set coordinates datum NAD83/MLLW		
latitude	Floating point starting with +/- or ending with (N or S). For example, +/-16.67 or 16.67N.	string	Maximum length: 15	
longitude	Floating point starting with +/- or ending with (N or S). For example, +/-26.789 or 26.789E.	string	Maximum length: 15	
parent-key	Parent key name.	string	Maximum length: 63	

### config elin-number

Parameter	Description	Type	Size	Default
elin-num	Configure ELIN callback number.	string	Maximum length: 31	
parent-key	Parent key name.	string	Maximum length: 63	

## config switch-controller mac-policy



This command is available for model(s): FortiGate 1000D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001E1, FortiGate 5001E.

Configure MAC policy to be applied on the managed FortiSwitch devices through NAC device.

```
config switch-controller mac-policy
    Description: Configure MAC policy to be applied on the managed FortiSwitch devices
    through NAC device.
    edit <name>
        set bounce-port-link [disable|enable]
        set count [disable|enable]
        set description {string}
        set fortilink {string}
        set traffic-policy {string}
        set vlan {string}
    next
end
```

## config switch-controller mac-policy

Parameter	Description	Type	Size	Default
bounce-port-link	Enable/disable bouncing (administratively bring the link down, up) of a switch port where this mac-policy is applied.	option	-	enable

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable bouncing (administratively bring the link down, up) of a switch port where this mac-policy is applied.		
	<i>enable</i>	Enable bouncing (administratively bring the link down, up) of a switch port where this mac-policy is applied.		
count	Enable/disable packet count on the NAC device.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Enable packet count on the NAC device.		
	<i>enable</i>	Disable packet count on the NAC device.		
description	Description for the MAC policy.	string	Maximum length: 63	
fortilink	FortiLink interface for which this MAC policy belongs to.	string	Maximum length: 15	
name	MAC policy name.	string	Maximum length: 63	
traffic-policy	Traffic policy to be applied when using this MAC policy.	string	Maximum length: 63	
vlan	Ingress traffic VLAN assignment for the MAC address matching this MAC policy.	string	Maximum length: 15	

## config switch-controller managed-switch



This command is available for model(s): FortiGate 1000D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3900E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001E1, FortiGate 5001E.

Configure FortiSwitch devices that are managed by this FortiGate.

```
config switch-controller managed-switch
  Description: Configure FortiSwitch devices that are managed by this FortiGate.
  edit <switch-id>
    config 802-1X-settings
      Description: Configuration method to edit FortiSwitch 802.1X global settings.
      set local-override [enable|disable]
      set link-down-auth [set-unauth|no-action]
      set reauth-period {integer}
      set max-reauth-attempt {integer}
      set tx-period {integer}
    end
    set access-profile {string}
    config custom-command
      Description: Configuration method to edit FortiSwitch commands to be pushed to
      this FortiSwitch device upon rebooting the FortiGate switch controller or the FortiSwitch.
      edit <command-entry>
        set command-name {string}
      next
    end
    set delayed-restart-trigger {integer}
    set description {string}
    set dhcp-server-access-list [global|enable|...]
    set directly-connected {integer}
    set dynamic-capability {user}
    set dynamically-discovered {integer}
```

```

set firmware-provision [enable|disable]
set firmware-provision-latest [disable|once]
set firmware-provision-version {string}
set flow-identity {user}
set fsw-wan1-admin [discovered|disable|...]
set fsw-wan1-peer {string}
config igmp-snooping
    Description: Configure FortiSwitch IGMP snooping global settings.
    set local-override [enable|disable]
    set aging-time {integer}
    set flood-unknown-multicast [enable|disable]
    config vlans
        Description: Configure IGMP snooping VLAN.
        edit <vlan-name>
            set proxy [disable|enable|...]
            set querier [disable|enable]
            set querier-addr {ipv4-address}
            set version {integer}
        next
    end
end
config ip-source-guard
    Description: IP source guard.
    edit <port>
        set description {string}
        config binding-entry
            Description: IP and MAC address configuration.
            edit <entry-name>
                set ip {ipv4-address-any}
                set mac {mac-address}
            next
        end
    next
end
set l3-discovered {integer}
set max-allowed-trunk-members {integer}
set mclag-igmp-snooping-aware [enable|disable]
config mirror
    Description: Configuration method to edit FortiSwitch packet mirror.
    edit <name>
        set status [active|inactive]
        set switching-packet [enable|disable]
        set dst {string}
        set src-ingress <name1>, <name2>, ...
        set src-egress <name1>, <name2>, ...
    next
end
set name {string}
set override-snmp-community [enable|disable]
set override-snmp-sysinfo [disable|enable]
set override-snmp-trap-threshold [enable|disable]
set override-snmp-user [enable|disable]
set owner-vdom {string}
set poe-detection-type {integer}
set poe-pre-standard-detection [enable|disable]
config ports

```



---

Description: Managed-switch port list.

```
edit <port-name>
    set port-owner {string}
    set switch-id {string}
    set speed [10half|10full|...]
    set status [up|down]
    set poe-status [enable|disable]
    set ip-source-guard [disable|enable]
    set ptp-policy {string}
    set aggregator-mode [bandwidth|count]
    set rpvt-port [disabled|enabled]
    set poe-pre-standard-detection [enable|disable]
    set port-number {integer}
    set port-prefix-type {integer}
    set fortilink-port {integer}
    set poe-capable {integer}
    set stacking-port {integer}
    set p2p-port {integer}
    set mclag-icl-port {integer}
    set fiber-port {integer}
    set media-type {string}
    set poe-standard {string}
    set poe-max-power {string}
    set flags {integer}
    set isl-local-trunk-name {string}
    set isl-peer-port-name {string}
    set isl-peer-device-name {string}
    set fgt-peer-port-name {string}
    set fgt-peer-device-name {string}
    set vlan {string}
    set allowed-vlans-all [enable|disable]
    set allowed-vlans <vlan-name1>, <vlan-name2>, ...
    set untagged-vlans <vlan-name1>, <vlan-name2>, ...
    set type [physical|trunk]
    set access-mode [dynamic|nac|...]
    set matched-dpp-policy {string}
    set matched-dpp-intf-tags {string}
    set dhcp-snooping [untrusted|trusted]
    set dhcp-snoop-option82-trust [enable|disable]
    set arp-inspection-trust [untrusted|trusted]
    set igmps-flood-reports [enable|disable]
    set igmps-flood-traffic [enable|disable]
    set stp-state [enabled|disabled]
    set stp-root-guard [enabled|disabled]
    set stp-bpdu-guard [enabled|disabled]
    set stp-bpdu-guard-timeout {integer}
    set edge-port [enable|disable]
    set discard-mode [none|all-untagged|...]
    set packet-sampler [enabled|disabled]
    set packet-sample-rate {integer}
    set sflow-counter-interval {integer}
    set sample-direction [tx|rx|...]
    set fec-capable {integer}
    set fec-state [disabled|cl74|...]
    set flow-control [disable|tx|...]
    set pause-meter {integer}
```

```

        set pause-meter-resume [75%|50%|...]
        set loop-guard [enabled|disabled]
        set loop-guard-timeout {integer}
        set port-policy {string}
        set qos-policy {string}
        set storm-control-policy {string}
        set port-security-policy {string}
        set export-to-pool {string}
        set interface-tags <tag-name1>, <tag-name2>, ...
        set learning-limit {integer}
        set sticky-mac [enable|disable]
        set lldp-status [disable|rx-only|...]
        set lldp-profile {string}
        set export-to {string}
        set mac-addr {mac-address}
        set port-selection-criteria [src-mac|dst-mac|...]
        set description {string}
        set lacp-speed [slow|fast]
        set mode [static|lacp-passive|...]
        set bundle [enable|disable]
        set member-withdrawal-behavior [forward|block]
        set mclag [enable|disable]
        set min-bundle {integer}
        set max-bundle {integer}
        set members <member-name1>, <member-name2>, ...
    next
end
set pre-provisioned {integer}
set qos-drop-policy [taildrop|random-early-detection]
set qos-red-probability {integer}
config remote-log
    Description: Configure logging by FortiSwitch device to a remote syslog server.
    edit <name>
        set status [enable|disable]
        set server {string}
        set port {integer}
        set severity [emergency|alert|...]
        set csv [enable|disable]
        set facility [kernel|user|...]
    next
end
config snmp-community
    Description: Configuration method to edit Simple Network Management Protocol
(SNMP) communities.
    edit <id>
        set name {string}
        set status [disable|enable]
        config hosts
            Description: Configure IPv4 SNMP managers (hosts).
            edit <id>
                set ip {user}
            next
        end
        set query-v1-status [disable|enable]
        set query-v1-port {integer}
        set query-v2c-status [disable|enable]

```

```

        set query-v2c-port {integer}
        set trap-v1-status [disable|enable]
        set trap-v1-lport {integer}
        set trap-v1-rport {integer}
        set trap-v2c-status [disable|enable]
        set trap-v2c-lport {integer}
        set trap-v2c-rport {integer}
        set events {option1}, {option2}, ...
    next
end
config snmp-sysinfo
    Description: Configuration method to edit Simple Network Management Protocol
(SNMP) system info.
    set status [disable|enable]
    set engine-id {string}
    set description {string}
    set contact-info {string}
    set location {string}
end
config snmp-trap-threshold
    Description: Configuration method to edit Simple Network Management Protocol
(SNMP) trap threshold values.
    set trap-high-cpu-threshold {integer}
    set trap-low-memory-threshold {integer}
    set trap-log-full-threshold {integer}
end
config snmp-user
    Description: Configuration method to edit Simple Network Management Protocol
(SNMP) users.
    edit <name>
        set queries [disable|enable]
        set query-port {integer}
        set security-level [no-auth-no-priv|auth-no-priv|...]
        set auth-proto [md5|sha1|...]
        set auth-pwd {password}
        set priv-proto [aes128|aes192|...]
        set priv-pwd {password}
    next
end
set staged-image-version {string}
config static-mac
    Description: Configuration method to edit FortiSwitch Static and Sticky MAC.
    edit <id>
        set type [static|sticky]
        set vlan {string}
        set mac {mac-address}
        set interface {string}
        set description {string}
    next
end
config storm-control
    Description: Configuration method to edit FortiSwitch storm control for
measuring traffic activity using data rates to prevent traffic disruption.
    set local-override [enable|disable]
    set rate {integer}
    set unknown-unicast [enable|disable]

```

```

        set unknown-multicast [enable|disable]
        set broadcast [enable|disable]
    end
    config stp-instance
        Description: Configuration method to edit Spanning Tree Protocol (STP)
instances.
        edit <id>
            set priority [0|4096|...]
        next
    end
    config stp-settings
        Description: Configuration method to edit Spanning Tree Protocol (STP) settings
used to prevent bridge loops.
        set local-override [enable|disable]
        set name {string}
        set revision {integer}
        set hello-time {integer}
        set forward-time {integer}
        set max-age {integer}
        set max-hops {integer}
        set pending-timer {integer}
    end
    set switch-device-tag {string}
    set switch-dhcp_opt43_key {string}
    config switch-log
        Description: Configuration method to edit FortiSwitch logging settings (logs are
transferred to and inserted into the FortiGate event log).
        set local-override [enable|disable]
        set status [enable|disable]
        set severity [emergency|alert|...]
    end
    set switch-profile {string}
    set tdr-supported {string}
    set type [virtual|physical]
    set version {integer}
next
end

```

## config switch-controller managed-switch

Parameter	Description	Type	Size	Default
access-profile	FortiSwitch access profile.	string	Maximum length: 31	default
delayed-restart-trigger	Delayed restart triggered for this FortiSwitch.	integer	Minimum value: 0 Maximum value: 255	0
description	Description.	string	Maximum length: 63	
dhcp-server-access-list	DHCP snooping server access list.	option	-	global

Parameter	Description	Type	Size	Default
	<b>Option</b>		<b>Description</b>	
	<i>global</i>	Use global setting for DHCP snooping server access list.		
	<i>enable</i>	Override global setting and enable DHCP server access list.		
	<i>disable</i>	Override global setting and disable DHCP server access list.		
directly-connected	Directly connected FortiSwitch.	integer	Minimum value: 0 Maximum value: 1	0
dynamic-capability	List of features this FortiSwitch supports (not configurable) that is sent to the FortiGate device for subsequent configuration initiated by the FortiGate device.	user	Not Specified	0x00000000000000000000000000000000
dynamically-discovered	Dynamically discovered FortiSwitch.	integer	Minimum value: 0 Maximum value: 1	0
firmware-provision	Enable/disable provisioning of firmware to FortiSwitches on join connection.	option	-	disable
	<b>Option</b>		<b>Description</b>	
	<i>enable</i>	Enable firmware-provision.		
	<i>disable</i>	Disable firmware-provision.		
firmware-provision-latest	Enable/disable one-time automatic provisioning of the latest firmware version.	option	-	disable
	<b>Option</b>		<b>Description</b>	
	<i>disable</i>	Do not automatically provision the latest available firmware.		
	<i>once</i>	Automatically attempt a one-time upgrade to the latest available firmware version.		

Parameter	Description	Type	Size	Default								
firmware-provision-version	Firmware version to provision to this FortiSwitch on bootup (major.minor.build, i.e. 6.2.1234).	string	Maximum length: 35									
flow-identity	Flow-tracking netflow ipfix switch identity in hex format.	user	Not Specified	00000000								
fsw-wan1-admin	FortiSwitch WAN1 admin status; enable to authorize the FortiSwitch as a managed switch.	option	-	discovered								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>discovered</td><td>Link waiting to be authorized.</td></tr><tr><td>disable</td><td>Link unauthorized.</td></tr><tr><td>enable</td><td>Link authorized.</td></tr></table>				Option	Description	discovered	Link waiting to be authorized.	disable	Link unauthorized.	enable	Link authorized.
Option	Description											
discovered	Link waiting to be authorized.											
disable	Link unauthorized.											
enable	Link authorized.											
fsw-wan1-peer	FortiSwitch WAN1 peer port.	string	Maximum length: 35									
l3-discovered	Layer 3 management discovered.	integer	Minimum value: 0 Maximum value: 1	0								
max-allowed-trunk-members	FortiSwitch maximum allowed trunk members.	integer	Minimum value: 0 Maximum value: 255	0								
mclag-igmp-snooping-aware	Enable/disable MCLAG IGMP-snooping awareness.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable MCLAG IGMP-snooping awareness.</td></tr><tr><td>disable</td><td>Disable MCLAG IGMP-snooping awareness.</td></tr></table>				Option	Description	enable	Enable MCLAG IGMP-snooping awareness.	disable	Disable MCLAG IGMP-snooping awareness.		
Option	Description											
enable	Enable MCLAG IGMP-snooping awareness.											
disable	Disable MCLAG IGMP-snooping awareness.											
name	Managed-switch name.	string	Maximum length: 35									

Parameter	Description	Type	Size	Default						
override-snmcommunity	Enable/disable overriding the global SNMP communities.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Override the global SNMP communities.</td></tr><tr><td><i>disable</i></td><td>Use the global SNMP communities.</td></tr></table>	Option	Description	<i>enable</i>	Override the global SNMP communities.	<i>disable</i>	Use the global SNMP communities.			
Option	Description									
<i>enable</i>	Override the global SNMP communities.									
<i>disable</i>	Use the global SNMP communities.									
override-snm-sysinfo	Enable/disable overriding the global SNMP system information.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Use the global SNMP system information.</td></tr><tr><td><i>enable</i></td><td>Override the global SNMP system information.</td></tr></table>	Option	Description	<i>disable</i>	Use the global SNMP system information.	<i>enable</i>	Override the global SNMP system information.			
Option	Description									
<i>disable</i>	Use the global SNMP system information.									
<i>enable</i>	Override the global SNMP system information.									
override-snm-trap-threshold	Enable/disable overriding the global SNMP trap threshold values.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Override the global SNMP trap threshold values.</td></tr><tr><td><i>disable</i></td><td>Use the global SNMP trap threshold values.</td></tr></table>	Option	Description	<i>enable</i>	Override the global SNMP trap threshold values.	<i>disable</i>	Use the global SNMP trap threshold values.			
Option	Description									
<i>enable</i>	Override the global SNMP trap threshold values.									
<i>disable</i>	Use the global SNMP trap threshold values.									
override-snm-user	Enable/disable overriding the global SNMP users.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Override the global SNMPv3 users.</td></tr><tr><td><i>disable</i></td><td>Use the global SNMPv3 users.</td></tr></table>	Option	Description	<i>enable</i>	Override the global SNMPv3 users.	<i>disable</i>	Use the global SNMPv3 users.			
Option	Description									
<i>enable</i>	Override the global SNMPv3 users.									
<i>disable</i>	Use the global SNMPv3 users.									
owner-vdom	VDOM which owner of port belongs to.	string	Maximum length: 31							
poe-detection-type	PoE detection type for FortiSwitch.	integer	Minimum value: 0 Maximum value: 255	0						

Parameter	Description	Type	Size	Default
poe-pre-standard-detection	Enable/disable PoE pre-standard detection.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable PoE pre-standard detection.		
	<i>disable</i>	Disable PoE pre-standard detection.		
pre-provisioned	Pre-provisioned managed switch.	integer	Minimum value: 0 Maximum value: 255	0
qos-drop-policy	Set QoS drop-policy.	option	-	taildrop
	<b>Option</b>	<b>Description</b>		
	<i>taildrop</i>	Taildrop policy.		
	<i>random-early-detection</i>	Random early detection drop policy.		
qos-red-probability	Set QoS RED/WRED drop probability.	integer	Minimum value: 0 Maximum value: 100	12
staged-image-version	Staged image version for FortiSwitch.	string	Maximum length: 127	
switch-device-tag	User definable label/tag.	string	Maximum length: 32	
switch-dhcp_opt43_key	DHCP option43 key.	string	Maximum length: 63	
switch-id	Managed-switch id.	string	Maximum length: 16	
switch-profile	FortiSwitch profile.	string	Maximum length: 35	default
tdr-supported	TDR supported.	string	Maximum length: 31	
type	Indication of switch type, physical or virtual.	option	-	physical



Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>virtual</i>	Switch is of type virtual.		
	<i>physical</i>	Switch is of type physical.		
version	FortiSwitch version.	integer	Minimum value: 0 Maximum value: 255	0

### config 802-1X-settings

Parameter	Description	Type	Size	Default
local-override	Enable to override global 802.1X settings on individual FortiSwitches.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Override global 802.1X settings.		
	<i>disable</i>	Use global 802.1X settings.		
link-down-auth	Authentication state to set if a link is down.	option	-	set-unauth
	<b>Option</b>	<b>Description</b>		
	<i>set-unauth</i>	Interface set to unauth when down. Reauthentication is needed.		
	<i>no-action</i>	Interface reauthentication is not needed.		
reauth-period	Reauthentication time interval.	integer	Minimum value: 0 Maximum value: 1440	60
max-reauth-attempt	Maximum number of authentication attempts.	integer	Minimum value: 0 Maximum value: 15	3
tx-period	802.1X Tx period.	integer	Minimum value: 4 Maximum value: 60	30

## config custom-command

Parameter	Description	Type	Size	Default
command-entry	List of FortiSwitch commands.	string	Maximum length: 35	
command-name	Names of commands to be pushed to this FortiSwitch device, as configured under config switch-controller custom-command.	string	Maximum length: 35	

## config igmp-snooping

Parameter	Description	Type	Size	Default						
local-override	Enable/disable overriding the global IGMP snooping configuration.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Override the global IGMP snooping configuration.</td></tr><tr><td><i>disable</i></td><td>Use the global IGMP snooping configuration.</td></tr></table>	Option	Description	<i>enable</i>	Override the global IGMP snooping configuration.	<i>disable</i>	Use the global IGMP snooping configuration.			
Option	Description									
<i>enable</i>	Override the global IGMP snooping configuration.									
<i>disable</i>	Use the global IGMP snooping configuration.									
aging-time	Maximum time to retain a multicast snooping entry for which no packets have been seen.	integer	Minimum value: 15 Maximum value: 3600	300						
flood-unknown-multicast	Enable/disable unknown multicast flooding.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable unknown multicast flooding.</td></tr><tr><td><i>disable</i></td><td>Disable unknown multicast flooding.</td></tr></table>	Option	Description	<i>enable</i>	Enable unknown multicast flooding.	<i>disable</i>	Disable unknown multicast flooding.			
Option	Description									
<i>enable</i>	Enable unknown multicast flooding.									
<i>disable</i>	Disable unknown multicast flooding.									

## config vlans

Parameter	Description	Type	Size	Default
vlan-name	List of FortiSwitch VLANs.	string	Maximum length: 15	default
proxy	IGMP snooping proxy for the VLAN interface.	option	-	global
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable IGMP snooping proxy on VLAN interface.		

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable IGMP snooping proxy on VLAN interface.		
	<i>global</i>	Use global setting for IGMP snooping proxy on VLAN interface.		
querier	Enable/disable IGMP snooping querier for the VLAN interface.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable IGMP snooping querier on VLAN interface.		
	<i>enable</i>	Enable IGMP snooping querier on VLAN interface.		
querier-addr	IGMP snooping querier address.	ipv4-address	Not Specified	0.0.0.0
version	IGMP snooping querying version.	integer	Minimum value: 2 Maximum value: 3	2

### config ip-source-guard

Parameter	Description	Type	Size	Default
port	Ingress interface to which source guard is bound.	string	Maximum length: 15	
description	Description.	string	Maximum length: 63	

### config binding-entry

Parameter	Description	Type	Size	Default
entry-name	Configure binding pair.	string	Maximum length: 16	
ip	Source IP for this rule.	ipv4-address-any	Not Specified	0.0.0.0
mac	MAC address for this rule.	mac-address	Not Specified	00:00:00:00:00:00

## config mirror

Parameter	Description	Type	Size	Default
name	Mirror name.	string	Maximum length: 63	
status	Active/inactive mirror configuration.	option	-	inactive
	<b>Option</b>	<b>Description</b>		
	<i>active</i>	Activate mirror configuration.		
	<i>inactive</i>	Deactivate mirror configuration.		
switching-packet	Enable/disable switching functionality when mirroring.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable switching functionality when mirroring.		
	<i>disable</i>	Disable switching functionality when mirroring.		
dst	Destination port.	string	Maximum length: 63	
src-ingress <name>	Source ingress interfaces. Interface name.	string	Maximum length: 79	
src-egress <name>	Source egress interfaces. Interface name.	string	Maximum length: 79	

## config ports

Parameter	Description	Type	Size	Default						
port-name	Switch port name.	string	Maximum length: 15							
port-owner	Switch port name.	string	Maximum length: 15							
switch-id	Switch id.	string	Maximum length: 16							
speed	Switch port speed; default and available settings depend on hardware.	option	-	auto						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>10half</td><td>10M half-duplex.</td></tr><tr><td>10full</td><td>10M full-duplex.</td></tr></table>				Option	Description	10half	10M half-duplex.	10full	10M full-duplex.
Option	Description									
10half	10M half-duplex.									
10full	10M full-duplex.									

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>100half</i>	100M half-duplex.		
	<i>100full</i>	100M full-duplex.		
	<i>1000auto</i>	Auto-negotiation (1G full-duplex only).		
	<i>1000full-fiber</i>	1G full-duplex (fiber SFPs only)		
	<i>1000full</i>	1G full-duplex		
	<i>10000full</i>	10G full-duplex		
	<i>40000full</i>	40G full-duplex		
	<i>auto</i>	Auto-negotiation.		
	<i>auto-module</i>	Auto Module.		
	<i>100FX-half</i>	100Mbps half-duplex.100Base-FX.		
	<i>100FX-full</i>	100Mbps full-duplex.100Base-FX.		
	<i>100000full</i>	100Gbps full-duplex.		
	<i>2500auto</i>	Auto-Negotiation (2.5Gbps Only).		
	<i>25000full</i>	25Gbps full-duplex.		
	<i>50000full</i>	50Gbps full-duplex.		
	<i>10000cr</i>	10Gbps copper interface.		
	<i>10000sr</i>	10Gbps SFI interface.		
	<i>100000sr4</i>	100Gbps SFI interface.		
	<i>100000cr4</i>	100Gbps copper interface.		
	<i>40000sr4</i>	40Gbps SFI interface.		
	<i>40000cr4</i>	40Gbps copper interface.		
	<i>25000cr</i>	25Gbps copper interface.		
	<i>25000sr</i>	25Gbps SFI interface.		
	<i>50000cr</i>	50Gbps copper interface.		
	<i>50000sr</i>	50Gbps SFI interface.		
<i>5000auto</i>	5Gbps full-duplex.			
status	Switch port admin status: up or down.	option	-	up

Parameter	Description	Type	Size	Default
	<b>Option</b> <b>Description</b>			
	<i>up</i>	Set admin status up.		
	<i>down</i>	Set admin status down.		
poe-status	Enable/disable PoE status.	option	-	enable
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Enable PoE status.		
	<i>disable</i>	Disable PoE status.		
ip-source-guard	Enable/disable IP source guard.	option	-	disable
	<b>Option</b> <b>Description</b>			
	<i>disable</i>	Disable IP source guard.		
	<i>enable</i>	Enable IP source guard.		
ptp-policy	PTP policy configuration.	string	Maximum length: 63	default
aggregator-mode	LACP member select mode.	option	-	bandwidth
	<b>Option</b> <b>Description</b>			
	<i>bandwidth</i>	Member selection based on largest total bandwidth of links of similar speed.		
	<i>count</i>	Member selection based on largest count of similar link speed.		
rpvst-port	Enable/disable inter-operability with rapid PVST on this interface.	option	-	disabled
	<b>Option</b> <b>Description</b>			
	<i>disabled</i>	Disable inter-operability with rapid PVST on this interface.		
	<i>enabled</i>	Enable inter-operability with rapid PVST on this interface.		
poe-pre-standard-detection	Enable/disable PoE pre-standard detection.	option	-	disable
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Enable PoE pre-standard detection.		
	<i>disable</i>	Disable PoE pre-standard detection.		

Parameter	Description	Type	Size	Default
port-number	Port number.	integer	Minimum value: 1 Maximum value: 64	0
port-prefix-type	Port prefix type.	integer	Minimum value: 0 Maximum value: 1	0
fortilink-port	FortiLink uplink port.	integer	Minimum value: 0 Maximum value: 1	0
poe-capable	PoE capable.	integer	Minimum value: 0 Maximum value: 1	0
stacking-port	Stacking port.	integer	Minimum value: 0 Maximum value: 1	0
p2p-port	General peer to peer tunnel port.	integer	Minimum value: 0 Maximum value: 1	0
mclag-icl-port	MCLAG-ICL port.	integer	Minimum value: 0 Maximum value: 1	0
fiber-port	Fiber-port.	integer	Minimum value: 0 Maximum value: 1	0
media-type	Media type.	string	Maximum length: 31	
poe-standard	PoE standard supported.	string	Maximum length: 63	
poe-max-power	PoE maximum power.	string	Maximum length: 35	

Parameter	Description	Type	Size	Default						
flags	Port properties flags.	integer	Minimum value: 0 Maximum value: 4294967295	0						
isl-local-trunk-name	ISL local trunk name.	string	Maximum length: 15							
isl-peer-port-name	ISL peer port name.	string	Maximum length: 15							
isl-peer-device-name	ISL peer device name.	string	Maximum length: 16							
fgt-peer-port-name	FGT peer port name.	string	Maximum length: 15							
fgt-peer-device-name	FGT peer device name.	string	Maximum length: 16							
vlan	Assign switch ports to a VLAN.	string	Maximum length: 15							
allowed-vlans-all	Enable/disable all defined vlans on this port.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable all defined VLANs on this port.</td></tr><tr><td><i>disable</i></td><td>Disable all defined VLANs on this port.</td></tr></table>				Option	Description	<i>enable</i>	Enable all defined VLANs on this port.	<i>disable</i>	Disable all defined VLANs on this port.
Option	Description									
<i>enable</i>	Enable all defined VLANs on this port.									
<i>disable</i>	Disable all defined VLANs on this port.									
allowed-vlans <vlan-name>	Configure switch port tagged VLANs. VLAN name.	string	Maximum length: 79							
untagged-vlans <vlan-name>	Configure switch port untagged VLANs. VLAN name.	string	Maximum length: 79							
type	Interface type: physical or trunk port.	option	-	physical						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>physical</i></td><td>Physical port.</td></tr><tr><td><i>trunk</i></td><td>Trunk port.</td></tr></table>				Option	Description	<i>physical</i>	Physical port.	<i>trunk</i>	Trunk port.
Option	Description									
<i>physical</i>	Physical port.									
<i>trunk</i>	Trunk port.									
access-mode	Access mode of the port.	option	-	static						



Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>dynamic</i></td><td>Dynamic mode.</td></tr><tr><td><i>nac</i></td><td>NAC mode.</td></tr><tr><td><i>static</i></td><td>Static mode.</td></tr></table>	Option	Description	<i>dynamic</i>	Dynamic mode.	<i>nac</i>	NAC mode.	<i>static</i>	Static mode.			
	Option	Description										
	<i>dynamic</i>	Dynamic mode.										
	<i>nac</i>	NAC mode.										
<i>static</i>	Static mode.											
matched-dpp-policy	Matched child policy in the dynamic port policy.	string	Maximum length: 63									
matched-dpp-intf-tags	Matched interface tags in the dynamic port policy.	string	Maximum length: 63									
dhcp-snooping	Trusted or untrusted DHCP-snooping interface.	option	-	untrusted								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>untrusted</i></td><td>Untrusted DHCP snooping interface.</td></tr><tr><td><i>trusted</i></td><td>Trusted DHCP snooping interface.</td></tr></table>	Option	Description	<i>untrusted</i>	Untrusted DHCP snooping interface.	<i>trusted</i>	Trusted DHCP snooping interface.					
	Option	Description										
	<i>untrusted</i>	Untrusted DHCP snooping interface.										
<i>trusted</i>	Trusted DHCP snooping interface.											
dhcp-snoop-option82-trust	Enable/disable allowance of DHCP with option-82 on untrusted interface.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable allowance of DHCP with option-82 on untrusted interface.</td></tr><tr><td><i>disable</i></td><td>Disable allowance of DHCP with option-82 on untrusted interface.</td></tr></table>	Option	Description	<i>enable</i>	Enable allowance of DHCP with option-82 on untrusted interface.	<i>disable</i>	Disable allowance of DHCP with option-82 on untrusted interface.					
	Option	Description										
	<i>enable</i>	Enable allowance of DHCP with option-82 on untrusted interface.										
<i>disable</i>	Disable allowance of DHCP with option-82 on untrusted interface.											
arp-inspection-trust	Trusted or untrusted dynamic ARP inspection.	option	-	untrusted								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>untrusted</i></td><td>Untrusted dynamic ARP inspection.</td></tr><tr><td><i>trusted</i></td><td>Trusted dynamic ARP inspection.</td></tr></table>	Option	Description	<i>untrusted</i>	Untrusted dynamic ARP inspection.	<i>trusted</i>	Trusted dynamic ARP inspection.					
	Option	Description										
	<i>untrusted</i>	Untrusted dynamic ARP inspection.										
<i>trusted</i>	Trusted dynamic ARP inspection.											
igmps-flood-reports	Enable/disable flooding of IGMP reports to this interface when igmp-snooping enabled.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable flooding of IGMP snooping reports to this interface.</td></tr><tr><td><i>disable</i></td><td>Disable flooding of IGMP snooping reports to this interface.</td></tr></table>	Option	Description	<i>enable</i>	Enable flooding of IGMP snooping reports to this interface.	<i>disable</i>	Disable flooding of IGMP snooping reports to this interface.					
	Option	Description										
	<i>enable</i>	Enable flooding of IGMP snooping reports to this interface.										
<i>disable</i>	Disable flooding of IGMP snooping reports to this interface.											
igmps-flood-traffic	Enable/disable flooding of IGMP snooping traffic to this interface.	option	-	disable								

Parameter	Description	Type	Size	Default
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Enable flooding of IGMP snooping traffic to this interface.		
	<i>disable</i>	Disable flooding of IGMP snooping traffic to this interface.		
stp-state	Enable/disable Spanning Tree Protocol (STP) on this interface.	option	-	enabled
	<b>Option</b> <b>Description</b>			
	<i>enabled</i>	Enable STP on this interface.		
	<i>disabled</i>	Disable STP on this interface.		
stp-root-guard	Enable/disable STP root guard on this interface.	option	-	disabled
	<b>Option</b> <b>Description</b>			
	<i>enabled</i>	Enable STP root-guard on this interface.		
	<i>disabled</i>	Disable STP root-guard on this interface.		
stp-bpdu-guard	Enable/disable STP BPDU guard on this interface.	option	-	disabled
	<b>Option</b> <b>Description</b>			
	<i>enabled</i>	Enable STP BPDU guard on this interface.		
	<i>disabled</i>	Disable STP BPDU guard on this interface.		
stp-bpdu-guard-timeout	BPDU Guard disabling protection.	integer	Minimum value: 0 Maximum value: 120	5
edge-port	Enable/disable this interface as an edge port, bridging connections between workstations and/or computers.	option	-	enable
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Enable this interface as an edge port.		
	<i>disable</i>	Disable this interface as an edge port.		
discard-mode	Configure discard mode for port.	option	-	none

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>Discard disabled.</td></tr><tr><td><i>all-untagged</i></td><td>Discard all frames that are untagged.</td></tr><tr><td><i>all-tagged</i></td><td>Discard all frames that are tagged.</td></tr></table>		Option	Description	<i>none</i>	Discard disabled.	<i>all-untagged</i>	Discard all frames that are untagged.	<i>all-tagged</i>	Discard all frames that are tagged.		
	Option	Description										
	<i>none</i>	Discard disabled.										
	<i>all-untagged</i>	Discard all frames that are untagged.										
<i>all-tagged</i>	Discard all frames that are tagged.											
packet-sampler	Enable/disable packet sampling on this interface.	option	-	disabled								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enabled</i></td><td>Enable packet sampling on this interface.</td></tr><tr><td><i>disabled</i></td><td>Disable packet sampling on this interface.</td></tr></table>		Option	Description	<i>enabled</i>	Enable packet sampling on this interface.	<i>disabled</i>	Disable packet sampling on this interface.				
	Option	Description										
	<i>enabled</i>	Enable packet sampling on this interface.										
<i>disabled</i>	Disable packet sampling on this interface.											
packet-sample-rate	Packet sampling rate.	integer	Minimum value: 0 Maximum value: 99999	512								
sflow-counter-interval	sFlow sampling counter polling interval in seconds.	integer	Minimum value: 0 Maximum value: 255	0								
sample-direction	Packet sampling direction.	option	-	both								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>tx</i></td><td>Monitor transmitted traffic.</td></tr><tr><td><i>rx</i></td><td>Monitor received traffic.</td></tr><tr><td><i>both</i></td><td>Monitor transmitted and received traffic.</td></tr></table>		Option	Description	<i>tx</i>	Monitor transmitted traffic.	<i>rx</i>	Monitor received traffic.	<i>both</i>	Monitor transmitted and received traffic.		
	Option	Description										
	<i>tx</i>	Monitor transmitted traffic.										
	<i>rx</i>	Monitor received traffic.										
<i>both</i>	Monitor transmitted and received traffic.											
fec-capable	FEC capable.	integer	Minimum value: 0 Maximum value: 1	0								
fec-state	State of forward error correction.	option	-	cl91								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disabled</i></td><td>Disable forward error correction.</td></tr><tr><td><i>cl74</i></td><td>Enable Clause 74 FC-FEC, which only applies to 25Gbps.</td></tr><tr><td><i>cl91</i></td><td>Enable Clause 91 RS-FEC, which only applies to 100Gbps.</td></tr></table>		Option	Description	<i>disabled</i>	Disable forward error correction.	<i>cl74</i>	Enable Clause 74 FC-FEC, which only applies to 25Gbps.	<i>cl91</i>	Enable Clause 91 RS-FEC, which only applies to 100Gbps.		
	Option	Description										
	<i>disabled</i>	Disable forward error correction.										
	<i>cl74</i>	Enable Clause 74 FC-FEC, which only applies to 25Gbps.										
<i>cl91</i>	Enable Clause 91 RS-FEC, which only applies to 100Gbps.											

Parameter	Description	Type	Size	Default										
flow-control	Flow control direction.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable flow control.</td></tr><tr><td><i>tx</i></td><td>Enable flow control for transmission pause control frames.</td></tr><tr><td><i>rx</i></td><td>Enable flow control for receive pause control frames.</td></tr><tr><td><i>both</i></td><td>Enable flow control for both transmission and receive pause control frames.</td></tr></table>	Option	Description	<i>disable</i>	Disable flow control.	<i>tx</i>	Enable flow control for transmission pause control frames.	<i>rx</i>	Enable flow control for receive pause control frames.	<i>both</i>	Enable flow control for both transmission and receive pause control frames.			
	Option	Description												
	<i>disable</i>	Disable flow control.												
	<i>tx</i>	Enable flow control for transmission pause control frames.												
	<i>rx</i>	Enable flow control for receive pause control frames.												
<i>both</i>	Enable flow control for both transmission and receive pause control frames.													
pause-meter	Configure ingress pause metering rate, in kbps.	integer	Minimum value: 128 Maximum value: 2147483647	0										
pause-meter-resume	Resume threshold for resuming traffic on ingress port.	option	-	50%										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>75%</i></td><td>Back pressure state won't be cleared until bucket count falls below 75% of pause threshold.</td></tr><tr><td><i>50%</i></td><td>Back pressure state won't be cleared until bucket count falls below 50% of pause threshold.</td></tr><tr><td><i>25%</i></td><td>Back pressure state won't be cleared until bucket count falls below 25% of pause threshold.</td></tr></table>	Option	Description	<i>75%</i>	Back pressure state won't be cleared until bucket count falls below 75% of pause threshold.	<i>50%</i>	Back pressure state won't be cleared until bucket count falls below 50% of pause threshold.	<i>25%</i>	Back pressure state won't be cleared until bucket count falls below 25% of pause threshold.					
	Option	Description												
	<i>75%</i>	Back pressure state won't be cleared until bucket count falls below 75% of pause threshold.												
	<i>50%</i>	Back pressure state won't be cleared until bucket count falls below 50% of pause threshold.												
<i>25%</i>	Back pressure state won't be cleared until bucket count falls below 25% of pause threshold.													
loop-guard	Enable/disable loop-guard on this interface, an STP optimization used to prevent network loops.	option	-	disabled										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enabled</i></td><td>Enable loop-guard on this interface.</td></tr><tr><td><i>disabled</i></td><td>Disable loop-guard on this interface.</td></tr></table>	Option	Description	<i>enabled</i>	Enable loop-guard on this interface.	<i>disabled</i>	Disable loop-guard on this interface.							
	Option	Description												
	<i>enabled</i>	Enable loop-guard on this interface.												
<i>disabled</i>	Disable loop-guard on this interface.													
loop-guard-timeout	Loop-guard timeout.	integer	Minimum value: 0 Maximum value: 120	45										
port-policy	Switch controller dynamic port policy from available options.	string	Maximum length: 63											
qos-policy	Switch controller QoS policy from available options.	string	Maximum length: 63	default										

Parameter	Description	Type	Size	Default										
storm-control-policy	Switch controller storm control policy from available options.	string	Maximum length: 63	default										
port-security-policy	Switch controller authentication policy to apply to this managed switch from available options.	string	Maximum length: 31											
export-to-pool	Switch controller export port to pool-list.	string	Maximum length: 35											
interface-tags <tag-name>	Tag(s) associated with the interface for various features including virtual port pool, dynamic port policy. FortiSwitch port tag name when exported to a virtual port pool or matched to dynamic port policy.	string	Maximum length: 63											
learning-limit	Limit the number of dynamic MAC addresses on this Port.	integer	Minimum value: 0 Maximum value: 128	0										
sticky-mac	Enable or disable sticky-mac on the interface.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable sticky mac on the interface.</td></tr><tr><td><i>disable</i></td><td>Disable sticky mac on the interface.</td></tr></table>				Option	Description	<i>enable</i>	Enable sticky mac on the interface.	<i>disable</i>	Disable sticky mac on the interface.				
Option	Description													
<i>enable</i>	Enable sticky mac on the interface.													
<i>disable</i>	Disable sticky mac on the interface.													
lldp-status	LLDP transmit and receive status.	option	-	tx-rx										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable LLDP TX and RX.</td></tr><tr><td><i>rx-only</i></td><td>Enable LLDP as RX only.</td></tr><tr><td><i>tx-only</i></td><td>Enable LLDP as TX only.</td></tr><tr><td><i>tx-rx</i></td><td>Enable LLDP TX and RX.</td></tr></table>				Option	Description	<i>disable</i>	Disable LLDP TX and RX.	<i>rx-only</i>	Enable LLDP as RX only.	<i>tx-only</i>	Enable LLDP as TX only.	<i>tx-rx</i>	Enable LLDP TX and RX.
Option	Description													
<i>disable</i>	Disable LLDP TX and RX.													
<i>rx-only</i>	Enable LLDP as RX only.													
<i>tx-only</i>	Enable LLDP as TX only.													
<i>tx-rx</i>	Enable LLDP TX and RX.													
lldp-profile	LLDP port TLV profile.	string	Maximum length: 63	default-auto-isl										
export-to	Export managed-switch port to a tenant VDOM.	string	Maximum length: 31											
mac-addr	Port/Trunk MAC.	mac-address	Not Specified	00:00:00:00:00:00										

Parameter	Description	Type	Size	Default														
port-selection-criteria	Algorithm for aggregate port selection.	option	-	src-dst-ip														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>src-mac</td><td>Source MAC address.</td></tr><tr><td>dst-mac</td><td>Destination MAC address.</td></tr><tr><td>src-dst-mac</td><td>Source and destination MAC address.</td></tr><tr><td>src-ip</td><td>Source IP address.</td></tr><tr><td>dst-ip</td><td>Destination IP address.</td></tr><tr><td>src-dst-ip</td><td>Source and destination IP address.</td></tr></table>	Option	Description	src-mac	Source MAC address.	dst-mac	Destination MAC address.	src-dst-mac	Source and destination MAC address.	src-ip	Source IP address.	dst-ip	Destination IP address.	src-dst-ip	Source and destination IP address.			
Option	Description																	
src-mac	Source MAC address.																	
dst-mac	Destination MAC address.																	
src-dst-mac	Source and destination MAC address.																	
src-ip	Source IP address.																	
dst-ip	Destination IP address.																	
src-dst-ip	Source and destination IP address.																	
description	Description for port.	string	Maximum length: 63															
lacp-speed	End Link Aggregation Control Protocol (LACP) messages every 30 seconds (slow) or every second (fast).	option	-	slow														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>slow</td><td>Send LACP message every 30 seconds.</td></tr><tr><td>fast</td><td>Send LACP message every second.</td></tr></table>	Option	Description	slow	Send LACP message every 30 seconds.	fast	Send LACP message every second.											
Option	Description																	
slow	Send LACP message every 30 seconds.																	
fast	Send LACP message every second.																	
mode	LACP mode: ignore and do not send control messages, or negotiate 802.3ad aggregation passively or actively.	option	-	static														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>static</td><td>Static aggregation, do not send and ignore any control messages.</td></tr><tr><td>lacp-passive</td><td>Passively use LACP to negotiate 802.3ad aggregation.</td></tr><tr><td>lacp-active</td><td>Actively use LACP to negotiate 802.3ad aggregation.</td></tr></table>	Option	Description	static	Static aggregation, do not send and ignore any control messages.	lacp-passive	Passively use LACP to negotiate 802.3ad aggregation.	lacp-active	Actively use LACP to negotiate 802.3ad aggregation.									
Option	Description																	
static	Static aggregation, do not send and ignore any control messages.																	
lacp-passive	Passively use LACP to negotiate 802.3ad aggregation.																	
lacp-active	Actively use LACP to negotiate 802.3ad aggregation.																	
bundle	Enable/disable Link Aggregation Group (LAG) bundling for non-FortiLink interfaces.	option	-	disable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable bundling.</td></tr><tr><td>disable</td><td>Disable bundling.</td></tr></table>	Option	Description	enable	Enable bundling.	disable	Disable bundling.											
Option	Description																	
enable	Enable bundling.																	
disable	Disable bundling.																	

Parameter	Description	Type	Size	Default						
member-withdrawal-behavior	Port behavior after it withdraws because of loss of control packets.	option	-	block						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>forward</i></td><td>Forward traffic.</td></tr><tr><td><i>block</i></td><td>Block traffic.</td></tr></table>	Option	Description	<i>forward</i>	Forward traffic.	<i>block</i>	Block traffic.			
	Option	Description								
	<i>forward</i>	Forward traffic.								
<i>block</i>	Block traffic.									
mclag	Enable/disable multi-chassis link aggregation (MCLAG).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable MCLAG.</td></tr><tr><td><i>disable</i></td><td>Disable MCLAG.</td></tr></table>	Option	Description	<i>enable</i>	Enable MCLAG.	<i>disable</i>	Disable MCLAG.			
	Option	Description								
	<i>enable</i>	Enable MCLAG.								
<i>disable</i>	Disable MCLAG.									
min-bundle	Minimum size of LAG bundle.	integer	Minimum value: 1 Maximum value: 24	1						
max-bundle	Maximum size of LAG bundle.	integer	Minimum value: 1 Maximum value: 24	24						
members <member-name>	Aggregated LAG bundle interfaces. Interface name from available options.	string	Maximum length: 79							

### config remote-log

Parameter	Description	Type	Size	Default						
name	Remote log name.	string	Maximum length: 35							
status	Enable/disable logging by FortiSwitch device to a remote syslog server.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable logging by FortiSwitch device to a remote syslog server.</td></tr><tr><td><i>disable</i></td><td>Disable logging by FortiSwitch device to a remote syslog server.</td></tr></table>				Option	Description	<i>enable</i>	Enable logging by FortiSwitch device to a remote syslog server.	<i>disable</i>	Disable logging by FortiSwitch device to a remote syslog server.
Option	Description									
<i>enable</i>	Enable logging by FortiSwitch device to a remote syslog server.									
<i>disable</i>	Disable logging by FortiSwitch device to a remote syslog server.									
server	IPv4 address of the remote syslog server.	string	Maximum length: 63							

Parameter	Description	Type	Size	Default																				
port	Remote syslog server listening port.	integer	Minimum value: 0 Maximum value: 65535	514																				
severity	Severity of logs to be transferred to remote log server.	option	-	information																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>emergency</i></td><td>Emergency level.</td></tr><tr><td><i>alert</i></td><td>Alert level.</td></tr><tr><td><i>critical</i></td><td>Critical level.</td></tr><tr><td><i>error</i></td><td>Error level.</td></tr><tr><td><i>warning</i></td><td>Warning level.</td></tr><tr><td><i>notification</i></td><td>Notification level.</td></tr><tr><td><i>information</i></td><td>Information level.</td></tr><tr><td><i>debug</i></td><td>Debug level.</td></tr></table>	Option	Description	<i>emergency</i>	Emergency level.	<i>alert</i>	Alert level.	<i>critical</i>	Critical level.	<i>error</i>	Error level.	<i>warning</i>	Warning level.	<i>notification</i>	Notification level.	<i>information</i>	Information level.	<i>debug</i>	Debug level.					
	Option	Description																						
	<i>emergency</i>	Emergency level.																						
	<i>alert</i>	Alert level.																						
	<i>critical</i>	Critical level.																						
	<i>error</i>	Error level.																						
	<i>warning</i>	Warning level.																						
	<i>notification</i>	Notification level.																						
	<i>information</i>	Information level.																						
<i>debug</i>	Debug level.																							
csv	Enable/disable comma-separated value (CSV) strings.	option	-	disable																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable comma-separated value (CSV) strings.</td></tr><tr><td><i>disable</i></td><td>Disable comma-separated value (CSV) strings.</td></tr></table>	Option	Description	<i>enable</i>	Enable comma-separated value (CSV) strings.	<i>disable</i>	Disable comma-separated value (CSV) strings.																	
	Option	Description																						
	<i>enable</i>	Enable comma-separated value (CSV) strings.																						
<i>disable</i>	Disable comma-separated value (CSV) strings.																							
facility	Facility to log to remote syslog server.	option	-	local7																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>kernel</i></td><td>Kernel messages.</td></tr><tr><td><i>user</i></td><td>Random user-level messages.</td></tr><tr><td><i>mail</i></td><td>Mail system.</td></tr><tr><td><i>daemon</i></td><td>System daemons.</td></tr><tr><td><i>auth</i></td><td>Security/authorization messages.</td></tr><tr><td><i>syslog</i></td><td>Messages generated internally by syslogd.</td></tr><tr><td><i>lpr</i></td><td>Line printer subsystem.</td></tr><tr><td><i>news</i></td><td>Network news subsystem.</td></tr><tr><td><i>uucp</i></td><td>UUCP server messages.</td></tr></table>	Option	Description	<i>kernel</i>	Kernel messages.	<i>user</i>	Random user-level messages.	<i>mail</i>	Mail system.	<i>daemon</i>	System daemons.	<i>auth</i>	Security/authorization messages.	<i>syslog</i>	Messages generated internally by syslogd.	<i>lpr</i>	Line printer subsystem.	<i>news</i>	Network news subsystem.	<i>uucp</i>	UUCP server messages.			
	Option	Description																						
	<i>kernel</i>	Kernel messages.																						
	<i>user</i>	Random user-level messages.																						
	<i>mail</i>	Mail system.																						
	<i>daemon</i>	System daemons.																						
	<i>auth</i>	Security/authorization messages.																						
	<i>syslog</i>	Messages generated internally by syslogd.																						
	<i>lpr</i>	Line printer subsystem.																						
<i>news</i>	Network news subsystem.																							
<i>uucp</i>	UUCP server messages.																							



Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>cron</i>	Clock daemon.		
	<i>authpriv</i>	Security/authorization messages (private).		
	<i>ftp</i>	FTP daemon.		
	<i>ntp</i>	NTP daemon.		
	<i>audit</i>	Log audit.		
	<i>alert</i>	Log alert.		
	<i>clock</i>	Clock daemon.		
	<i>local0</i>	Reserved for local use.		
	<i>local1</i>	Reserved for local use.		
	<i>local2</i>	Reserved for local use.		
	<i>local3</i>	Reserved for local use.		
	<i>local4</i>	Reserved for local use.		
	<i>local5</i>	Reserved for local use.		
	<i>local6</i>	Reserved for local use.		
	<i>local7</i>	Reserved for local use.		

### config snmp-community

Parameter	Description	Type	Size	Default
id	SNMP community ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
name	SNMP community name.	string	Maximum length: 35	
status	Enable/disable this SNMP community.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable SNMP community.		
	<i>enable</i>	Enable SNMP community.		
query-v1-status	Enable/disable SNMP v1 queries.	option	-	enable

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable SNMP v1 queries.		
	<i>enable</i>	Enable SNMP v1 queries.		
query-v1-port	SNMP v1 query port.	integer	Minimum value: 0 Maximum value: 65535	161
query-v2c-status	Enable/disable SNMP v2c queries.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable SNMP v2c queries.		
	<i>enable</i>	Enable SNMP v2c queries.		
query-v2c-port	SNMP v2c query port.	integer	Minimum value: 0 Maximum value: 65535	161
trap-v1-status	Enable/disable SNMP v1 traps.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable SNMP v1 traps.		
	<i>enable</i>	Enable SNMP v1 traps.		
trap-v1-lport	SNMP v2c trap local port.	integer	Minimum value: 0 Maximum value: 65535	162
trap-v1-rport	SNMP v2c trap remote port.	integer	Minimum value: 0 Maximum value: 65535	162
trap-v2c-status	Enable/disable SNMP v2c traps.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable SNMP v2c traps.		
	<i>enable</i>	Enable SNMP v2c traps.		

Parameter	Description	Type	Size	Default
trap-v2c-lport	SNMP v2c trap local port.	integer	Minimum value: 0 Maximum value: 65535	162
trap-v2c-rport	SNMP v2c trap remote port.	integer	Minimum value: 0 Maximum value: 65535	162
events	SNMP notifications (traps) to send.	option	-	cpu-high mem-low log-full intf-ip ent-conf-change
		Option	Description	
		<i>cpu-high</i>	Send a trap when CPU usage too high.	
		<i>mem-low</i>	Send a trap when available memory is low.	
		<i>log-full</i>	Send a trap when log disk space becomes low.	
		<i>intf-ip</i>	Send a trap when an interface IP address is changed.	
		<i>ent-conf-change</i>	Send a trap when an entity MIB change occurs (RFC4133).	

### config hosts

Parameter	Description	Type	Size	Default
id	Host entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
ip	IPv4 address of the SNMP manager (host).	user	Not Specified	

### config snmp-sysinfo

Parameter	Description	Type	Size	Default
status	Enable/disable SNMP.	option	-	disable
		Option	Description	
		<i>disable</i>	Disable SNMP.	
		<i>enable</i>	Enable SNMP.	

Parameter	Description	Type	Size	Default
engine-id	Local SNMP engine ID string (max 24 char).	string	Maximum length: 24	
description	System description.	string	Maximum length: 35	
contact-info	Contact information.	string	Maximum length: 35	
location	System location.	string	Maximum length: 35	

### config snmp-trap-threshold

Parameter	Description	Type	Size	Default
trap-high-cpu-threshold	CPU usage when trap is sent.	integer	Minimum value: 0 Maximum value: 4294967295	80
trap-low-memory-threshold	Memory usage when trap is sent.	integer	Minimum value: 0 Maximum value: 4294967295	80
trap-log-full-threshold	Log disk usage when trap is sent.	integer	Minimum value: 0 Maximum value: 4294967295	90

### config snmp-user

Parameter	Description	Type	Size	Default						
name	SNMP user name.	string	Maximum length: 32							
queries	Enable/disable SNMP queries for this user.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable SNMP queries for this user.</td></tr><tr><td><i>enable</i></td><td>Enable SNMP queries for this user.</td></tr></table>				Option	Description	<i>disable</i>	Disable SNMP queries for this user.	<i>enable</i>	Enable SNMP queries for this user.
Option	Description									
<i>disable</i>	Disable SNMP queries for this user.									
<i>enable</i>	Enable SNMP queries for this user.									

Parameter	Description	Type	Size	Default
query-port	SNMPv3 query port.	integer	Minimum value: 0 Maximum value: 65535	161
security-level	Security level for message authentication and encryption.	option	-	no-auth-no-priv
	<b>Option</b>	<b>Description</b>		
	<i>no-auth-no-priv</i>	Message with no authentication and no privacy (encryption).		
	<i>auth-no-priv</i>	Message with authentication but no privacy (encryption).		
	<i>auth-priv</i>	Message with authentication and privacy (encryption).		
auth-proto	Authentication protocol.	option	-	sha256
	<b>Option</b>	<b>Description</b>		
	<i>md5</i>	HMAC-MD5-96 authentication protocol.		
	<i>sha1</i>	HMAC-SHA-1 authentication protocol.		
	<i>sha224</i>	HMAC-SHA-224 authentication protocol.		
	<i>sha256</i>	HMAC-SHA-256 authentication protocol.		
	<i>sha384</i>	HMAC-SHA-384 authentication protocol.		
	<i>sha512</i>	HMAC-SHA-512 authentication protocol.		
auth-pwd	Password for authentication protocol.	password	Not Specified	
priv-proto	Privacy (encryption) protocol.	option	-	aes128
	<b>Option</b>	<b>Description</b>		
	<i>aes128</i>	CFB128-AES-128 symmetric encryption protocol.		
	<i>aes192</i>	CFB128-AES-192 symmetric encryption protocol.		
	<i>aes192c</i>	CFB128-AES-192-C symmetric encryption protocol.		
	<i>aes256</i>	CFB128-AES-256 symmetric encryption protocol.		
	<i>aes256c</i>	CFB128-AES-256-C symmetric encryption protocol.		
	<i>des</i>	CBC-DES symmetric encryption protocol.		
priv-pwd	Password for privacy (encryption) protocol.	password	Not Specified	

## config static-mac

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
type	Type.	option	-	static
	<div>OptionDescription</div>			
	static	Static MAC.		
	sticky	Sticky MAC.		
vlan	Vlan.	string	Maximum length: 15	
mac	MAC address.	mac-address	Not Specified	00:00:00:00:00:00
interface	Interface name.	string	Maximum length: 35	
description	Description.	string	Maximum length: 63	

## config storm-control

Parameter	Description	Type	Size	Default
local-override	Enable to override global FortiSwitch storm control settings for this FortiSwitch.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Override global storm control settings.		
	<i>disable</i>	Use global storm control settings.		
rate	Rate in packets per second at which storm traffic is controlled. Storm control drops excess traffic data rates beyond this threshold.	integer	Minimum value: 1 Maximum value: 10000000	500
unknown-unicast	Enable/disable storm control to drop unknown unicast traffic.	option	-	disable

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Drop unknown unicast traffic.		
	<i>disable</i>	Allow unknown unicast traffic.		
unknown-multicast	Enable/disable storm control to drop unknown multicast traffic.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Drop unknown multicast traffic.		
	<i>disable</i>	Allow unknown multicast traffic.		
broadcast	Enable/disable storm control to drop broadcast traffic.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Drop broadcast traffic.		
	<i>disable</i>	Allow broadcast traffic.		

### config stp-instance

Parameter	Description	Type	Size	Default
id	Instance ID.	string	Maximum length: 2	
priority	Priority.	option	-	32768
	<b>Option</b>	<b>Description</b>		
	<i>0</i>	0.		
	<i>4096</i>	4096.		
	<i>8192</i>	8192.		
	<i>12288</i>	12288.		
	<i>16384</i>	16384.		
	<i>20480</i>	20480.		
	<i>24576</i>	24576.		
	<i>28672</i>	28672.		
	<i>32768</i>	32768.		
	<i>36864</i>	36864.		

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	40960	40960.		
	45056	45056.		
	49152	49152.		
	53248	53248.		
	57344	57344.		
	61440	61440.		

### config stp-settings

Parameter	Description	Type	Size	Default
local-override	Enable to configure local STP settings that override global STP settings.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Override global STP settings.		
	<i>disable</i>	Use global STP settings.		
name	Name of local STP settings configuration.	string	Maximum length: 31	
revision	STP revision number.	integer	Minimum value: 0 Maximum value: 65535	0
hello-time	Period of time between successive STP frame Bridge Protocol Data Units.	integer	Minimum value: 1 Maximum value: 10	2
forward-time	Period of time a port is in listening and learning state.	integer	Minimum value: 4 Maximum value: 30	15
max-age	Maximum time before a bridge port saves its configuration BPDU information.	integer	Minimum value: 6 Maximum value: 40	20



Parameter	Description	Type	Size	Default
max-hops	Maximum number of hops between the root bridge and the furthest bridge.	integer	Minimum value: 1 Maximum value: 40	20
pending-timer	Pending time.	integer	Minimum value: 1 Maximum value: 15	4

## config switch-log

Parameter	Description	Type	Size	Default																		
local-override	Enable to configure local logging settings that override global logging settings.	option	-	disable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Override global logging settings.</td></tr><tr><td><i>disable</i></td><td>Use global logging settings.</td></tr></table>	Option	Description	<i>enable</i>	Override global logging settings.	<i>disable</i>	Use global logging settings.															
Option	Description																					
<i>enable</i>	Override global logging settings.																					
<i>disable</i>	Use global logging settings.																					
status	Enable/disable adding FortiSwitch logs to the FortiGate event log.	option	-	enable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Add FortiSwitch logs to the FortiGate event log.</td></tr><tr><td><i>disable</i></td><td>Do not add FortiSwitch logs to the FortiGate event log.</td></tr></table>	Option	Description	<i>enable</i>	Add FortiSwitch logs to the FortiGate event log.	<i>disable</i>	Do not add FortiSwitch logs to the FortiGate event log.															
Option	Description																					
<i>enable</i>	Add FortiSwitch logs to the FortiGate event log.																					
<i>disable</i>	Do not add FortiSwitch logs to the FortiGate event log.																					
severity	Severity of FortiSwitch logs that are added to the FortiGate event log.	option	-	notification																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>emergency</i></td><td>Emergency level.</td></tr><tr><td><i>alert</i></td><td>Alert level.</td></tr><tr><td><i>critical</i></td><td>Critical level.</td></tr><tr><td><i>error</i></td><td>Error level.</td></tr><tr><td><i>warning</i></td><td>Warning level.</td></tr><tr><td><i>notification</i></td><td>Notification level.</td></tr><tr><td><i>information</i></td><td>Information level.</td></tr><tr><td><i>debug</i></td><td>Debug level.</td></tr></table>	Option	Description	<i>emergency</i>	Emergency level.	<i>alert</i>	Alert level.	<i>critical</i>	Critical level.	<i>error</i>	Error level.	<i>warning</i>	Warning level.	<i>notification</i>	Notification level.	<i>information</i>	Information level.	<i>debug</i>	Debug level.			
Option	Description																					
<i>emergency</i>	Emergency level.																					
<i>alert</i>	Alert level.																					
<i>critical</i>	Critical level.																					
<i>error</i>	Error level.																					
<i>warning</i>	Warning level.																					
<i>notification</i>	Notification level.																					
<i>information</i>	Information level.																					
<i>debug</i>	Debug level.																					

## config switch-controller network-monitor-settings



This command is available for model(s): FortiGate 1000D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001E1, FortiGate 5001E.

Configure network monitor settings.

```
config switch-controller network-monitor-settings
    Description: Configure network monitor settings.
    set network-monitoring [enable|disable]
end
```

## config switch-controller network-monitor-settings

Parameter	Description	Type	Size	Default						
network-monitoring	Enable/disable passive gathering of information by FortiSwitch units concerning other network devices.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable network monitoring on FortiSwitch.</td></tr><tr><td><i>disable</i></td><td>Disable network monitoring on FortiSwitch.</td></tr></table>	Option	Description	<i>enable</i>	Enable network monitoring on FortiSwitch.	<i>disable</i>	Disable network monitoring on FortiSwitch.			
Option	Description									
<i>enable</i>	Enable network monitoring on FortiSwitch.									
<i>disable</i>	Disable network monitoring on FortiSwitch.									

## config switch-controller ptp policy



This command is available for model(s): FortiGate 1000D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001E1, FortiGate 5001E.

PTP policy configuration.

```
config switch-controller ptp policy
    Description: PTP policy configuration.
    edit <name>
        set status [disable|enable]
    next
end
```

## config switch-controller ptp policy

Parameter	Description	Type	Size	Default
name	Policy name.	string	Maximum length: 63	
status	Enable/disable PTP policy.	option	-	enable
		Option	Description	
		<i>disable</i>	Disable PTP policy.	
		<i>enable</i>	Enable PTP policy.	

## config switch-controller ptp settings



This command is available for model(s): FortiGate 1000D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001E1, FortiGate 5001E.

Global PTP settings.

```
config switch-controller ptp settings
    Description: Global PTP settings.
    set mode [disable|transparent-e2e|...]
end
```

## config switch-controller ptp settings

Parameter	Description	Type	Size	Default
mode	Enable/disable PTP mode.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable PTP function. Packets are forwarded with no action.		
	<i>transparent-e2e</i>	Enable end-to-end transparent clock.		
	<i>transparent-p2p</i>	Enable peer-to-peer transparent clock.		

## config switch-controller qos dot1p-map



This command is available for model(s): FortiGate 1000D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001E1, FortiGate 5001E.

### Configure FortiSwitch QoS 802.1p.

```
config switch-controller qos dot1p-map
  Description: Configure FortiSwitch QoS 802.1p.
  edit <name>
    set description {string}
    set egress-pri-tagging [disable|enable]
    set priority-0 [queue-0|queue-1|...]
    set priority-1 [queue-0|queue-1|...]
    set priority-2 [queue-0|queue-1|...]
    set priority-3 [queue-0|queue-1|...]
    set priority-4 [queue-0|queue-1|...]
    set priority-5 [queue-0|queue-1|...]
    set priority-6 [queue-0|queue-1|...]
    set priority-7 [queue-0|queue-1|...]
  next
end
```

## config switch-controller qos dot1p-map

Parameter	Description	Type	Size	Default
description	Description of the 802.1p name.	string	Maximum length: 63	

Parameter	Description	Type	Size	Default
egress-pri-tagging	Enable/disable egress priority-tag frame.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable egress priority tagging.		
	<i>enable</i>	Enable egress priority tagging.		
name	Dot1p map name.	string	Maximum length: 63	
priority-0	COS queue mapped to dot1p priority number.	option	-	queue-0
	<b>Option</b>	<b>Description</b>		
	<i>queue-0</i>	COS queue 0 (lowest priority).		
	<i>queue-1</i>	COS queue 1.		
	<i>queue-2</i>	COS queue 2.		
	<i>queue-3</i>	COS queue 3.		
	<i>queue-4</i>	COS queue 4.		
	<i>queue-5</i>	COS queue 5.		
	<i>queue-6</i>	COS queue 6.		
	<i>queue-7</i>	COS queue 7 (highest priority).		
priority-1	COS queue mapped to dot1p priority number.	option	-	queue-0
	<b>Option</b>	<b>Description</b>		
	<i>queue-0</i>	COS queue 0 (lowest priority).		
	<i>queue-1</i>	COS queue 1.		
	<i>queue-2</i>	COS queue 2.		
	<i>queue-3</i>	COS queue 3.		
	<i>queue-4</i>	COS queue 4.		
	<i>queue-5</i>	COS queue 5.		
	<i>queue-6</i>	COS queue 6.		
	<i>queue-7</i>	COS queue 7 (highest priority).		
priority-2	COS queue mapped to dot1p priority number.	option	-	queue-0

Parameter	Description	Type	Size	Default
	Option	Description		
	queue-0	COS queue 0 (lowest priority).		
	queue-1	COS queue 1.		
	queue-2	COS queue 2.		
	queue-3	COS queue 3.		
	queue-4	COS queue 4.		
	queue-5	COS queue 5.		
	queue-6	COS queue 6.		
	queue-7	COS queue 7 (highest priority).		
priority-3	COS queue mapped to dot1p priority number.	option	-	queue-0
	Option	Description		
	queue-0	COS queue 0 (lowest priority).		
	queue-1	COS queue 1.		
	queue-2	COS queue 2.		
	queue-3	COS queue 3.		
	queue-4	COS queue 4.		
	queue-5	COS queue 5.		
	queue-6	COS queue 6.		
	queue-7	COS queue 7 (highest priority).		
priority-4	COS queue mapped to dot1p priority number.	option	-	queue-0
	Option	Description		
	queue-0	COS queue 0 (lowest priority).		
	queue-1	COS queue 1.		
	queue-2	COS queue 2.		
	queue-3	COS queue 3.		
	queue-4	COS queue 4.		
	queue-5	COS queue 5.		
	queue-6	COS queue 6.		
	queue-7	COS queue 7 (highest priority).		

Parameter	Description	Type	Size	Default
priority-5	COS queue mapped to dot1p priority number.	option	-	queue-0
	<b>Option</b>	<b>Description</b>		
	<i>queue-0</i>	COS queue 0 (lowest priority).		
	<i>queue-1</i>	COS queue 1.		
	<i>queue-2</i>	COS queue 2.		
	<i>queue-3</i>	COS queue 3.		
	<i>queue-4</i>	COS queue 4.		
	<i>queue-5</i>	COS queue 5.		
	<i>queue-6</i>	COS queue 6.		
	<i>queue-7</i>	COS queue 7 (highest priority).		
priority-6	COS queue mapped to dot1p priority number.	option	-	queue-0
	<b>Option</b>	<b>Description</b>		
	<i>queue-0</i>	COS queue 0 (lowest priority).		
	<i>queue-1</i>	COS queue 1.		
	<i>queue-2</i>	COS queue 2.		
	<i>queue-3</i>	COS queue 3.		
	<i>queue-4</i>	COS queue 4.		
	<i>queue-5</i>	COS queue 5.		
	<i>queue-6</i>	COS queue 6.		
	<i>queue-7</i>	COS queue 7 (highest priority).		
priority-7	COS queue mapped to dot1p priority number.	option	-	queue-0
	<b>Option</b>	<b>Description</b>		
	<i>queue-0</i>	COS queue 0 (lowest priority).		
	<i>queue-1</i>	COS queue 1.		
	<i>queue-2</i>	COS queue 2.		
	<i>queue-3</i>	COS queue 3.		
	<i>queue-4</i>	COS queue 4.		
	<i>queue-5</i>	COS queue 5.		
	<i>queue-6</i>	COS queue 6.		
	<i>queue-7</i>	COS queue 7 (highest priority).		



## config switch-controller qos ip-dscp-map



This command is available for model(s): FortiGate 1000D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001E1, FortiGate 5001E.

Configure FortiSwitch QoS IP precedence/DSCP.

```
config switch-controller qos ip-dscp-map
  Description: Configure FortiSwitch QoS IP precedence/DSCP.
  edit <name>
    set description {string}
    config map
      Description: Maps between IP-DSCP value to COS queue.
      edit <name>
        set cos-queue {integer}
        set diffserv {option1}, {option2}, ...
        set ip-precedence {option1}, {option2}, ...
        set value {user}
      next
    end
  next
end
```

## config switch-controller qos ip-dscp-map

Parameter	Description	Type	Size	Default
description	Description of the ip-dscp map name.	string	Maximum length: 63	

Parameter	Description	Type	Size	Default
name	Dscp map name.	string	Maximum length: 63	

## config map

Parameter	Description	Type	Size	Default
name	Dscp mapping entry name.	string	Maximum length: 63	
cos-queue	COS queue number.	integer	Minimum value: 0 Maximum value: 7	0
diffserv	Differentiated service.	option	-	

Option	Description
CS0	DSCP CS0.
CS1	DSCP CS1.
AF11	DSCP AF11.
AF12	DSCP AF12.
AF13	DSCP AF13.
CS2	DSCP CS2.
AF21	DSCP AF21.
AF22	DSCP AF22.
AF23	DSCP AF23.
CS3	DSCP CS3.
AF31	DSCP AF31.
AF32	DSCP AF32.
AF33	DSCP AF33.
CS4	DSCP CS4.
AF41	DSCP AF41.
AF42	DSCP AF42.
AF43	DSCP AF43.
CS5	DSCP CS5.
EF	DSCP EF.

Parameter	Description	Type	Size	Default																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>CS6</td><td>DSCP CS6.</td></tr><tr><td>CS7</td><td>DSCP CS7.</td></tr></table>	Option	Description	CS6	DSCP CS6.	CS7	DSCP CS7.															
	Option	Description																				
	CS6	DSCP CS6.																				
CS7	DSCP CS7.																					
ip-precedence	IP Precedence.	option	-																			
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>network-control</i></td><td>Network control.</td></tr><tr><td><i>internetwork-control</i></td><td>Internetwork control.</td></tr><tr><td><i>critic-ecp</i></td><td>Critic ECP.</td></tr><tr><td><i>flashoverride</i></td><td>Flash override.</td></tr><tr><td><i>flash</i></td><td>Flash.</td></tr><tr><td><i>immediate</i></td><td>Immediate.</td></tr><tr><td><i>priority</i></td><td>Priority.</td></tr><tr><td><i>routine</i></td><td>Routine.</td></tr></table>	Option	Description	<i>network-control</i>	Network control.	<i>internetwork-control</i>	Internetwork control.	<i>critic-ecp</i>	Critic ECP.	<i>flashoverride</i>	Flash override.	<i>flash</i>	Flash.	<i>immediate</i>	Immediate.	<i>priority</i>	Priority.	<i>routine</i>	Routine.			
	Option	Description																				
	<i>network-control</i>	Network control.																				
	<i>internetwork-control</i>	Internetwork control.																				
	<i>critic-ecp</i>	Critic ECP.																				
	<i>flashoverride</i>	Flash override.																				
	<i>flash</i>	Flash.																				
	<i>immediate</i>	Immediate.																				
	<i>priority</i>	Priority.																				
<i>routine</i>	Routine.																					
value	Raw values of DSCP.	user	Not Specified																			

## config switch-controller qos qos-policy



This command is available for model(s): FortiGate 1000D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3900E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001E1, FortiGate 5001E.

Configure FortiSwitch QoS policy.

```
config switch-controller qos qos-policy
  Description: Configure FortiSwitch QoS policy.
  edit <name>
    set default-cos {integer}
    set queue-policy {string}
    set trust-dot1p-map {string}
    set trust-ip-dscp-map {string}
  next
end
```

## config switch-controller qos qos-policy

Parameter	Description	Type	Size	Default
default-cos	Default cos queue for untagged packets.	integer	Minimum value: 0 Maximum value: 7	0
name	QoS policy name.	string	Maximum length: 63	

Parameter	Description	Type	Size	Default
queue-policy	QoS egress queue policy.	string	Maximum length: 63	default
trust-dot1p-map	QoS trust 802.1p map.	string	Maximum length: 63	
trust-ip-dscp-map	QoS trust ip dscp map.	string	Maximum length: 63	

## config switch-controller qos queue-policy



This command is available for model(s): FortiGate 1000D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001E1, FortiGate 5001E.

Configure FortiSwitch QoS egress queue policy.

```
config switch-controller qos queue-policy
    Description: Configure FortiSwitch QoS egress queue policy.
    edit <name>
        config cos-queue
            Description: COS queue configuration.
            edit <name>
                set description {string}
                set min-rate {integer}
                set max-rate {integer}
                set min-rate-percent {integer}
                set max-rate-percent {integer}
                set drop-policy [taildrop|weighted-random-early-detection]
                set ecn [disable|enable]
```

```

        set weight {integer}
    next
end
set rate-by [kbps|percent]
set schedule [strict|round-robin|...]
next
end

```

## config switch-controller qos queue-policy

Parameter	Description	Type	Size	Default								
name	QoS policy name.	string	Maximum length: 63									
rate-by	COS queue rate by kbps or percent.	option	-	kbps								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>kbps</i></td><td>Rate by kbps.</td></tr><tr><td><i>percent</i></td><td>Rate by percent.</td></tr></table>	Option	Description	<i>kbps</i>	Rate by kbps.	<i>percent</i>	Rate by percent.					
Option	Description											
<i>kbps</i>	Rate by kbps.											
<i>percent</i>	Rate by percent.											
schedule	COS queue scheduling.	option	-	round-robin								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>strict</i></td><td>Strict scheduling (queue7: highest priority, queue0: lowest priority).</td></tr><tr><td><i>round-robin</i></td><td>Round robin scheduling.</td></tr><tr><td><i>weighted</i></td><td>Weighted round robin scheduling.</td></tr></table>	Option	Description	<i>strict</i>	Strict scheduling (queue7: highest priority, queue0: lowest priority).	<i>round-robin</i>	Round robin scheduling.	<i>weighted</i>	Weighted round robin scheduling.			
Option	Description											
<i>strict</i>	Strict scheduling (queue7: highest priority, queue0: lowest priority).											
<i>round-robin</i>	Round robin scheduling.											
<i>weighted</i>	Weighted round robin scheduling.											

## config cos-queue

Parameter	Description	Type	Size	Default
name	Cos queue ID.	string	Maximum length: 63	
description	Description of the COS queue.	string	Maximum length: 63	
min-rate	Minimum rate.	integer	Minimum value: 0 Maximum value: 4294967295	0

Parameter	Description	Type	Size	Default						
max-rate	Maximum rate.	integer	Minimum value: 0 Maximum value: 4294967295	0						
min-rate-percent	Minimum rate (% of link speed).	integer	Minimum value: 0 Maximum value: 4294967295	0						
max-rate-percent	Maximum rate (% of link speed).	integer	Minimum value: 0 Maximum value: 4294967295	0						
drop-policy	COS queue drop policy.	option	-	taildrop						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>taildrop</i></td><td>Taildrop policy.</td></tr><tr><td><i>weighted-random-early-detection</i></td><td>Weighted random early detection drop policy.</td></tr></table>				Option	Description	<i>taildrop</i>	Taildrop policy.	<i>weighted-random-early-detection</i>	Weighted random early detection drop policy.
Option	Description									
<i>taildrop</i>	Taildrop policy.									
<i>weighted-random-early-detection</i>	Weighted random early detection drop policy.									
ecn	Enable/disable ECN packet marking to drop eligible packets.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable ECN packet marking to drop eligible packets.</td></tr><tr><td><i>enable</i></td><td>Enable ECN packet marking to drop eligible packets.</td></tr></table>				Option	Description	<i>disable</i>	Disable ECN packet marking to drop eligible packets.	<i>enable</i>	Enable ECN packet marking to drop eligible packets.
Option	Description									
<i>disable</i>	Disable ECN packet marking to drop eligible packets.									
<i>enable</i>	Enable ECN packet marking to drop eligible packets.									
weight	Weight of weighted round robin scheduling.	integer	Minimum value: 0 Maximum value: 4294967295	1						

## config switch-controller quarantine



This command is available for model(s): FortiGate 1000D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001E1, FortiGate 5001E.

Configure FortiSwitch quarantine support.

```
config switch-controller quarantine
  Description: Configure FortiSwitch quarantine support.
  set quarantine [enable|disable]
  config targets
    Description: Quarantine MACs.
    edit <mac>
      set description {string}
      set tag <tags1>, <tags2>, ...
    next
  end
end
```

## config switch-controller quarantine

Parameter	Description	Type	Size	Default
quarantine	Enable/disable quarantine.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable quarantine.		
	<i>disable</i>	Disable quarantine.		



## config targets

Parameter	Description	Type	Size	Default
mac	Quarantine MAC.	mac-address	Not Specified	00:00:00:00:00:00
description	Description for the quarantine MAC.	string	Maximum length: 63	
tag <tags>	Tags for the quarantine MAC. Tag string. For example, string1 string2 string3.	string	Maximum length: 63	

## config switch-controller remote-log



This command is available for model(s): FortiGate 1000D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001E1, FortiGate 5001E.

Configure logging by FortiSwitch device to a remote syslog server.

```
config switch-controller remote-log
  Description: Configure logging by FortiSwitch device to a remote syslog server.
  edit <name>
    set csv [enable|disable]
    set facility [kernel|user|...]
    set port {integer}
    set server {string}
    set severity [emergency|alert|...]
    set status [enable|disable]
```

next  
end

## config switch-controller remote-log

Parameter	Description	Type	Size	Default
csv	Enable/disable comma-separated value (CSV) strings.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable comma-separated value (CSV) strings.		
	<i>disable</i>	Disable comma-separated value (CSV) strings.		
facility	Facility to log to remote syslog server.	option	-	local7
	<b>Option</b>	<b>Description</b>		
	<i>kernel</i>	Kernel messages.		
	<i>user</i>	Random user-level messages.		
	<i>mail</i>	Mail system.		
	<i>daemon</i>	System daemons.		
	<i>auth</i>	Security/authorization messages.		
	<i>syslog</i>	Messages generated internally by syslogd.		
	<i>lpr</i>	Line printer subsystem.		
	<i>news</i>	Network news subsystem.		
	<i>uucp</i>	UUCP server messages.		
	<i>cron</i>	Clock daemon.		
	<i>authpriv</i>	Security/authorization messages (private).		
	<i>ftp</i>	FTP daemon.		
	<i>ntp</i>	NTP daemon.		
	<i>audit</i>	Log audit.		
	<i>alert</i>	Log alert.		
	<i>clock</i>	Clock daemon.		
	<i>local0</i>	Reserved for local use.		
	<i>local1</i>	Reserved for local use.		
	<i>local2</i>	Reserved for local use.		
	<i>local3</i>	Reserved for local use.		

Parameter	Description	Type	Size	Default																			
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>local4</i></td><td>Reserved for local use.</td></tr><tr><td><i>local5</i></td><td>Reserved for local use.</td></tr><tr><td><i>local6</i></td><td>Reserved for local use.</td></tr><tr><td><i>local7</i></td><td>Reserved for local use.</td></tr></table>		Option	Description	<i>local4</i>	Reserved for local use.	<i>local5</i>	Reserved for local use.	<i>local6</i>	Reserved for local use.	<i>local7</i>	Reserved for local use.											
	Option	Description																					
	<i>local4</i>	Reserved for local use.																					
	<i>local5</i>	Reserved for local use.																					
	<i>local6</i>	Reserved for local use.																					
<i>local7</i>	Reserved for local use.																						
name	Remote log name.	string	Maximum length: 35																				
port	Remote syslog server listening port.	integer	Minimum value: 0 Maximum value: 65535	514																			
server	IPv4 address of the remote syslog server.	string	Maximum length: 63																				
severity	Severity of logs to be transferred to remote log server.	option	-	information																			
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>emergency</i></td><td>Emergency level.</td></tr><tr><td><i>alert</i></td><td>Alert level.</td></tr><tr><td><i>critical</i></td><td>Critical level.</td></tr><tr><td><i>error</i></td><td>Error level.</td></tr><tr><td><i>warning</i></td><td>Warning level.</td></tr><tr><td><i>notification</i></td><td>Notification level.</td></tr><tr><td><i>information</i></td><td>Information level.</td></tr><tr><td><i>debug</i></td><td>Debug level.</td></tr></table>		Option	Description	<i>emergency</i>	Emergency level.	<i>alert</i>	Alert level.	<i>critical</i>	Critical level.	<i>error</i>	Error level.	<i>warning</i>	Warning level.	<i>notification</i>	Notification level.	<i>information</i>	Information level.	<i>debug</i>	Debug level.			
	Option	Description																					
	<i>emergency</i>	Emergency level.																					
	<i>alert</i>	Alert level.																					
	<i>critical</i>	Critical level.																					
	<i>error</i>	Error level.																					
	<i>warning</i>	Warning level.																					
	<i>notification</i>	Notification level.																					
	<i>information</i>	Information level.																					
<i>debug</i>	Debug level.																						
status	Enable/disable logging by FortiSwitch device to a remote syslog server.	option	-	disable																			
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable logging by FortiSwitch device to a remote syslog server.</td></tr><tr><td><i>disable</i></td><td>Disable logging by FortiSwitch device to a remote syslog server.</td></tr></table>		Option	Description	<i>enable</i>	Enable logging by FortiSwitch device to a remote syslog server.	<i>disable</i>	Disable logging by FortiSwitch device to a remote syslog server.															
	Option	Description																					
	<i>enable</i>	Enable logging by FortiSwitch device to a remote syslog server.																					
<i>disable</i>	Disable logging by FortiSwitch device to a remote syslog server.																						

---

## config switch-controller security-policy 802-1X

---



This command is available for model(s): FortiGate 1000D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001E1, FortiGate 5001E.

---

### Configure 802.1x MAC Authentication Bypass (MAB) policies.

```
config switch-controller security-policy 802-1X
  Description: Configure 802.1x MAC Authentication Bypass (MAB) policies.
  edit <name>
    set auth-fail-vlan [disable|enable]
    set auth-fail-vlan-id {string}
    set authserver-timeout-period {integer}
    set authserver-timeout-vlan [disable|enable]
    set authserver-timeout-vlanid {string}
    set eap-auto-untagged-vlans [disable|enable]
    set eap-passthru [disable|enable]
    set framevid-apply [disable|enable]
    set guest-auth-delay {integer}
    set guest-vlan [disable|enable]
    set guest-vlan-id {string}
    set mac-auth-bypass [disable|enable]
    set open-auth [disable|enable]
    set policy-type {option}
    set radius-timeout-overwrite [disable|enable]
    set security-mode [802.1X|802.1X-mac-based]
    set user-group <name1>, <name2>, ...
  next
end
```

## config switch-controller security-policy 802-1X

Parameter	Description	Type	Size	Default						
auth-fail-vlan	Enable to allow limited access to clients that cannot authenticate.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable authentication fail VLAN on this interface.</td></tr><tr><td><i>enable</i></td><td>Enable authentication fail VLAN on this interface.</td></tr></table>	Option	Description	<i>disable</i>	Disable authentication fail VLAN on this interface.	<i>enable</i>	Enable authentication fail VLAN on this interface.			
Option	Description									
<i>disable</i>	Disable authentication fail VLAN on this interface.									
<i>enable</i>	Enable authentication fail VLAN on this interface.									
auth-fail-vlan-id	VLAN ID on which authentication failed.	string	Maximum length: 15							
authserver-timeout-period	Authentication server timeout period.	integer	Minimum value: 3 Maximum value: 15	3						
authserver-timeout-vlan	Enable/disable the authentication server timeout VLAN to allow limited access when RADIUS is unavailable.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable authentication server timeout VLAN on this interface.</td></tr><tr><td><i>enable</i></td><td>Enable authentication server timeout VLAN on this interface.</td></tr></table>	Option	Description	<i>disable</i>	Disable authentication server timeout VLAN on this interface.	<i>enable</i>	Enable authentication server timeout VLAN on this interface.			
Option	Description									
<i>disable</i>	Disable authentication server timeout VLAN on this interface.									
<i>enable</i>	Enable authentication server timeout VLAN on this interface.									
authserver-timeout-vlanid	Authentication server timeout VLAN name.	string	Maximum length: 15							
eap-auto-untagged-vlans	Enable/disable automatic inclusion of untagged VLANs.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable automatic inclusion of untagged VLANs.</td></tr><tr><td><i>enable</i></td><td>Enable automatic inclusion of untagged VLANs.</td></tr></table>	Option	Description	<i>disable</i>	Disable automatic inclusion of untagged VLANs.	<i>enable</i>	Enable automatic inclusion of untagged VLANs.			
Option	Description									
<i>disable</i>	Disable automatic inclusion of untagged VLANs.									
<i>enable</i>	Enable automatic inclusion of untagged VLANs.									
eap-passthru	Enable/disable EAP pass-through mode, allowing protocols (such as LLDP) to pass through ports for more flexible authentication.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable EAP pass-through mode on this interface.</td></tr><tr><td><i>enable</i></td><td>Enable EAP pass-through mode on this interface.</td></tr></table>	Option	Description	<i>disable</i>	Disable EAP pass-through mode on this interface.	<i>enable</i>	Enable EAP pass-through mode on this interface.			
Option	Description									
<i>disable</i>	Disable EAP pass-through mode on this interface.									
<i>enable</i>	Enable EAP pass-through mode on this interface.									
framevid-apply	Enable/disable the capability to apply the EAP/MAB frame VLAN to the port native VLAN.	option	-	enable						

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable the capability to apply the EAP/MAB frame VLAN to the port native VLAN.		
	<i>enable</i>	Enable the capability to apply the EAP/MAB frame VLAN to the port native VLAN.		
guest-auth-delay	Guest authentication delay.	integer	Minimum value: 1 Maximum value: 900	30
guest-vlan	Enable the guest VLAN feature to allow limited access to non-802.1X-compliant clients.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable guest VLAN on this interface.		
	<i>enable</i>	Enable guest VLAN on this interface.		
guest-vlan-id	Guest VLAN name.	string	Maximum length: 15	
mac-auth-bypass	Enable/disable MAB for this policy.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable MAB.		
	<i>enable</i>	Enable MAB.		
name	Policy name.	string	Maximum length: 31	
open-auth	Enable/disable open authentication for this policy.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable open authentication.		
	<i>enable</i>	Enable open authentication.		
policy-type	Policy type.	option	-	802.1X
	<b>Option</b>	<b>Description</b>		
	<i>802.1X</i>	802.1X security policy.		

Parameter	Description	Type	Size	Default						
radius-timeout-overwrite	Enable to override the global RADIUS session timeout.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Override the global RADIUS session timeout.</td></tr><tr><td><i>enable</i></td><td>Use the global RADIUS session timeout.</td></tr></table>	Option	Description	<i>disable</i>	Override the global RADIUS session timeout.	<i>enable</i>	Use the global RADIUS session timeout.			
Option	Description									
<i>disable</i>	Override the global RADIUS session timeout.									
<i>enable</i>	Use the global RADIUS session timeout.									
security-mode	Port or MAC based 802.1X security mode.	option	-	802.1X						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>802.1X</i></td><td>802.1X port based authentication.</td></tr><tr><td><i>802.1X-mac-based</i></td><td>802.1X MAC based authentication.</td></tr></table>	Option	Description	<i>802.1X</i>	802.1X port based authentication.	<i>802.1X-mac-based</i>	802.1X MAC based authentication.			
Option	Description									
<i>802.1X</i>	802.1X port based authentication.									
<i>802.1X-mac-based</i>	802.1X MAC based authentication.									
user-group <name>	Name of user-group to assign to this MAC Authentication Bypass (MAB) policy. Group name.	string	Maximum length: 79							

## config switch-controller security-policy local-access



This command is available for model(s): FortiGate 1000D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001E1, FortiGate 5001E.

Configure allowaccess list for mgmt and internal interfaces on managed FortiSwitch units.

```
config switch-controller security-policy local-access
    Description: Configure allowaccess list for mgmt and internal interfaces on managed
FortiSwitch units.
    edit <name>
        set internal-allowaccess {option1}, {option2}, ...
        set mgmt-allowaccess {option1}, {option2}, ...
    next
end
```

## config switch-controller security-policy local-access

Parameter	Description	Type	Size	Default
internal-allowaccess	Allowed access on the switch internal interface.	option	-	https ping ssh
	Option	Description		
	https	HTTPS access.		
	ping	PING access.		
	ssh	SSH access.		
	snmp	SNMP access.		
	http	HTTP access.		
	telnet	TELNET access.		
	radius-acct	RADIUS accounting access.		
mgmt-allowaccess	Allowed access on the switch management interface.	option	-	https ping ssh
	Option	Description		
	https	HTTPS access.		
	ping	PING access.		
	ssh	SSH access.		
	snmp	SNMP access.		
	http	HTTP access.		
	telnet	TELNET access.		
	radius-acct	RADIUS accounting access.		
name	Policy name.	string	Maximum length: 31	



## config switch-controller sflow



This command is available for model(s): FortiGate 1000D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001E1, FortiGate 5001E.

Configure FortiSwitch sFlow.

```
config switch-controller sflow
    Description: Configure FortiSwitch sFlow.
    set collector-ip {ipv4-address}
    set collector-port {integer}
end
```

## config switch-controller sflow

Parameter	Description	Type	Size	Default
collector-ip	Collector IP.	ipv4-address	Not Specified	0.0.0.0
collector-port	SFlow collector port.	integer	Minimum value: 0 Maximum value: 65535	6343

---

## config switch-controller snmp-community

---



This command is available for model(s): FortiGate 1000D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001E1, FortiGate 5001E.

---

Configure FortiSwitch SNMP v1/v2c communities globally.

```
config switch-controller snmp-community
  Description: Configure FortiSwitch SNMP v1/v2c communities globally.
  edit <id>
    set events {option1}, {option2}, ...
    config hosts
      Description: Configure IPv4 SNMP managers (hosts).
      edit <id>
        set ip {user}
      next
    end
    set name {string}
    set query-v1-port {integer}
    set query-v1-status [disable|enable]
    set query-v2c-port {integer}
    set query-v2c-status [disable|enable]
    set status [disable|enable]
    set trap-v1-lport {integer}
    set trap-v1-rport {integer}
    set trap-v1-status [disable|enable]
    set trap-v2c-lport {integer}
    set trap-v2c-rport {integer}
    set trap-v2c-status [disable|enable]
  next
end
```

## config switch-controller snmp-community

Parameter	Description	Type	Size	Default												
events	SNMP notifications (traps) to send.	option	-	cpu-high mem-low log-full intf- ip ent-conf- change												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>cpu-high</i></td><td>Send a trap when CPU usage too high.</td></tr><tr><td><i>mem-low</i></td><td>Send a trap when available memory is low.</td></tr><tr><td><i>log-full</i></td><td>Send a trap when log disk space becomes low.</td></tr><tr><td><i>intf-ip</i></td><td>Send a trap when an interface IP address is changed.</td></tr><tr><td><i>ent-conf-change</i></td><td>Send a trap when an entity MIB change occurs (RFC4133).</td></tr></table>	Option	Description	<i>cpu-high</i>	Send a trap when CPU usage too high.	<i>mem-low</i>	Send a trap when available memory is low.	<i>log-full</i>	Send a trap when log disk space becomes low.	<i>intf-ip</i>	Send a trap when an interface IP address is changed.	<i>ent-conf-change</i>	Send a trap when an entity MIB change occurs (RFC4133).			
Option	Description															
<i>cpu-high</i>	Send a trap when CPU usage too high.															
<i>mem-low</i>	Send a trap when available memory is low.															
<i>log-full</i>	Send a trap when log disk space becomes low.															
<i>intf-ip</i>	Send a trap when an interface IP address is changed.															
<i>ent-conf-change</i>	Send a trap when an entity MIB change occurs (RFC4133).															
id	SNMP community ID.	integer	Minimum value: 0 Maximum value: 4294967295	0												
name	SNMP community name.	string	Maximum length: 35													
query-v1-port	SNMP v1 query port.	integer	Minimum value: 0 Maximum value: 65535	161												
query-v1-status	Enable/disable SNMP v1 queries.	option	-	enable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable SNMP v1 queries.</td></tr><tr><td><i>enable</i></td><td>Enable SNMP v1 queries.</td></tr></table>	Option	Description	<i>disable</i>	Disable SNMP v1 queries.	<i>enable</i>	Enable SNMP v1 queries.									
Option	Description															
<i>disable</i>	Disable SNMP v1 queries.															
<i>enable</i>	Enable SNMP v1 queries.															
query-v2c-port	SNMP v2c query port.	integer	Minimum value: 0 Maximum value: 65535	161												
query-v2c-status	Enable/disable SNMP v2c queries.	option	-	enable												

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable SNMP v2c queries.		
	<i>enable</i>	Enable SNMP v2c queries.		
status	Enable/disable this SNMP community.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable SNMP community.		
	<i>enable</i>	Enable SNMP community.		
trap-v1-lport	SNMP v2c trap local port.	integer	Minimum value: 0 Maximum value: 65535	162
trap-v1-rport	SNMP v2c trap remote port.	integer	Minimum value: 0 Maximum value: 65535	162
trap-v1-status	Enable/disable SNMP v1 traps.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable SNMP v1 traps.		
	<i>enable</i>	Enable SNMP v1 traps.		
trap-v2c-lport	SNMP v2c trap local port.	integer	Minimum value: 0 Maximum value: 65535	162
trap-v2c-rport	SNMP v2c trap remote port.	integer	Minimum value: 0 Maximum value: 65535	162
trap-v2c-status	Enable/disable SNMP v2c traps.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable SNMP v2c traps.		
	<i>enable</i>	Enable SNMP v2c traps.		

## config hosts

Parameter	Description	Type	Size	Default
id	Host entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
ip	IPv4 address of the SNMP manager (host).	user	Not Specified	

## config switch-controller snmp-sysinfo



This command is available for model(s): FortiGate 1000D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001E1, FortiGate 5001E.

Configure FortiSwitch SNMP system information globally.

```
config switch-controller snmp-sysinfo
    Description: Configure FortiSwitch SNMP system information globally.
    set contact-info {string}
    set description {string}
    set engine-id {string}
    set location {string}
    set status [disable|enable]
end
```

## config switch-controller snmp-sysinfo

Parameter	Description	Type	Size	Default
contact-info	Contact information.	string	Maximum length: 35	
description	System description.	string	Maximum length: 35	
engine-id	Local SNMP engine ID string (max 24 char).	string	Maximum length: 24	
location	System location.	string	Maximum length: 35	
status	Enable/disable SNMP.	option	-	disable
		Option	Description	
		<i>disable</i>	Disable SNMP.	
		<i>enable</i>	Enable SNMP.	

## config switch-controller snmp-trap-threshold



This command is available for model(s): FortiGate 1000D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3900E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001E1, FortiGate 5001E.

Configure FortiSwitch SNMP trap threshold values globally.

```

config switch-controller snmp-trap-threshold
    Description: Configure FortiSwitch SNMP trap threshold values globally.
    set trap-high-cpu-threshold {integer}
    set trap-log-full-threshold {integer}
    set trap-low-memory-threshold {integer}
end

```

## config switch-controller snmp-trap-threshold

Parameter	Description	Type	Size	Default
trap-high-cpu-threshold	CPU usage when trap is sent.	integer	Minimum value: 0 Maximum value: 4294967295	80
trap-log-full-threshold	Log disk usage when trap is sent.	integer	Minimum value: 0 Maximum value: 4294967295	90
trap-low-memory-threshold	Memory usage when trap is sent.	integer	Minimum value: 0 Maximum value: 4294967295	80

## config switch-controller snmp-user



This command is available for model(s): FortiGate 1000D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001E1, FortiGate 5001E.

Configure FortiSwitch SNMP v3 users globally.

```
config switch-controller snmp-user
  Description: Configure FortiSwitch SNMP v3 users globally.
  edit <name>
    set auth-proto [md5|sha1|...]
    set auth-pwd {password}
    set priv-proto [aes128|aes192|...]
    set priv-pwd {password}
    set queries [disable|enable]
    set query-port {integer}
    set security-level [no-auth-no-priv|auth-no-priv|...]
  next
end
```

## config switch-controller snmp-user

Parameter	Description	Type	Size	Default				
auth-proto	Authentication protocol.	option	-	sha256				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>md5</td><td>HMAC-MD5-96 authentication protocol.</td></tr></table>	Option	Description	md5	HMAC-MD5-96 authentication protocol.			
Option	Description							
md5	HMAC-MD5-96 authentication protocol.							



Parameter	Description	Type	Size	Default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>sha1</td><td>HMAC-SHA-1 authentication protocol.</td></tr><tr><td>sha224</td><td>HMAC-SHA-224 authentication protocol.</td></tr><tr><td>sha256</td><td>HMAC-SHA-256 authentication protocol.</td></tr><tr><td>sha384</td><td>HMAC-SHA-384 authentication protocol.</td></tr><tr><td>sha512</td><td>HMAC-SHA-512 authentication protocol.</td></tr></table>	Option	Description	sha1	HMAC-SHA-1 authentication protocol.	sha224	HMAC-SHA-224 authentication protocol.	sha256	HMAC-SHA-256 authentication protocol.	sha384	HMAC-SHA-384 authentication protocol.	sha512	HMAC-SHA-512 authentication protocol.					
	Option	Description																
	sha1	HMAC-SHA-1 authentication protocol.																
	sha224	HMAC-SHA-224 authentication protocol.																
	sha256	HMAC-SHA-256 authentication protocol.																
	sha384	HMAC-SHA-384 authentication protocol.																
sha512	HMAC-SHA-512 authentication protocol.																	
auth-pwd	Password for authentication protocol.	password	Not Specified															
name	SNMP user name.	string	Maximum length: 32															
priv-proto	Privacy (encryption) protocol.	option	-	aes128														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>aes128</td><td>CFB128-AES-128 symmetric encryption protocol.</td></tr><tr><td>aes192</td><td>CFB128-AES-192 symmetric encryption protocol.</td></tr><tr><td>aes192c</td><td>CFB128-AES-192-C symmetric encryption protocol.</td></tr><tr><td>aes256</td><td>CFB128-AES-256 symmetric encryption protocol.</td></tr><tr><td>aes256c</td><td>CFB128-AES-256-C symmetric encryption protocol.</td></tr><tr><td>des</td><td>CBC-DES symmetric encryption protocol.</td></tr></table>	Option	Description	aes128	CFB128-AES-128 symmetric encryption protocol.	aes192	CFB128-AES-192 symmetric encryption protocol.	aes192c	CFB128-AES-192-C symmetric encryption protocol.	aes256	CFB128-AES-256 symmetric encryption protocol.	aes256c	CFB128-AES-256-C symmetric encryption protocol.	des	CBC-DES symmetric encryption protocol.			
	Option	Description																
	aes128	CFB128-AES-128 symmetric encryption protocol.																
	aes192	CFB128-AES-192 symmetric encryption protocol.																
	aes192c	CFB128-AES-192-C symmetric encryption protocol.																
	aes256	CFB128-AES-256 symmetric encryption protocol.																
	aes256c	CFB128-AES-256-C symmetric encryption protocol.																
des	CBC-DES symmetric encryption protocol.																	
priv-pwd	Password for privacy (encryption) protocol.	password	Not Specified															
queries	Enable/disable SNMP queries for this user.	option	-	enable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable SNMP queries for this user.</td></tr><tr><td>enable</td><td>Enable SNMP queries for this user.</td></tr></table>	Option	Description	disable	Disable SNMP queries for this user.	enable	Enable SNMP queries for this user.											
	Option	Description																
	disable	Disable SNMP queries for this user.																
enable	Enable SNMP queries for this user.																	
query-port	SNMPv3 query port.	integer	Minimum value: 0 Maximum value: 65535	161														
security-level	Security level for message authentication and encryption.	option	-	no-auth-no-priv														

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>no-auth-no-priv</i>	Message with no authentication and no privacy (encryption).		
	<i>auth-no-priv</i>	Message with authentication but no privacy (encryption).		
	<i>auth-priv</i>	Message with authentication and privacy (encryption).		

## config switch-controller storm-control-policy



This command is available for model(s): FortiGate 1000D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001E1, FortiGate 5001E.

Configure FortiSwitch storm control policy to be applied on managed-switch ports.

```
config switch-controller storm-control-policy
    Description: Configure FortiSwitch storm control policy to be applied on managed-switch
ports.
    edit <name>
        set broadcast [enable|disable]
        set description {string}
        set rate {integer}
        set storm-control-mode [global|override|...]
        set unknown-multicast [enable|disable]
        set unknown-unicast [enable|disable]
    next
end
```

## config switch-controller storm-control-policy

Parameter	Description	Type	Size	Default								
broadcast	Enable/disable storm control to drop/allow broadcast traffic in override mode.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable storm control for broadcast traffic to drop packets which exceed configured rate limits.</td></tr><tr><td><i>disable</i></td><td>Disable storm control for broadcast traffic to allow all packets.</td></tr></table>	Option	Description	<i>enable</i>	Enable storm control for broadcast traffic to drop packets which exceed configured rate limits.	<i>disable</i>	Disable storm control for broadcast traffic to allow all packets.					
Option	Description											
<i>enable</i>	Enable storm control for broadcast traffic to drop packets which exceed configured rate limits.											
<i>disable</i>	Disable storm control for broadcast traffic to allow all packets.											
description	Description of the storm control policy.	string	Maximum length: 63									
name	Storm control policy name.	string	Maximum length: 63									
rate	Threshold rate in packets per second at which storm traffic is controlled in override mode.	integer	Minimum value: 0 Maximum value: 10000000	500								
storm-control-mode	Set Storm control mode.	option	-	global								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>global</i></td><td>Apply Global or switch level storm control configuration.</td></tr><tr><td><i>override</i></td><td>Override global and switch level storm control to use port level configuration.</td></tr><tr><td><i>disabled</i></td><td>Disable storm control on the port entirely overriding global and switch level storm control.</td></tr></table>	Option	Description	<i>global</i>	Apply Global or switch level storm control configuration.	<i>override</i>	Override global and switch level storm control to use port level configuration.	<i>disabled</i>	Disable storm control on the port entirely overriding global and switch level storm control.			
Option	Description											
<i>global</i>	Apply Global or switch level storm control configuration.											
<i>override</i>	Override global and switch level storm control to use port level configuration.											
<i>disabled</i>	Disable storm control on the port entirely overriding global and switch level storm control.											
unknown-multicast	Enable/disable storm control to drop/allow unknown multicast traffic in override mode.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable storm control for unknown multicast traffic to drop packets which exceed configured rate limits.</td></tr><tr><td><i>disable</i></td><td>Disable storm control for unknown multicast traffic to allow all packets.</td></tr></table>	Option	Description	<i>enable</i>	Enable storm control for unknown multicast traffic to drop packets which exceed configured rate limits.	<i>disable</i>	Disable storm control for unknown multicast traffic to allow all packets.					
Option	Description											
<i>enable</i>	Enable storm control for unknown multicast traffic to drop packets which exceed configured rate limits.											
<i>disable</i>	Disable storm control for unknown multicast traffic to allow all packets.											
unknown-unicast	Enable/disable storm control to drop/allow unknown unicast traffic in override mode.	option	-	disable								

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable storm control for unknown unicast traffic to drop packets which exceed configured rate limits.		
	<i>disable</i>	Disable storm control for unknown unicast traffic to allow all packets.		

## config switch-controller storm-control



This command is available for model(s): FortiGate 1000D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001E1, FortiGate 5001E.

Configure FortiSwitch storm control.

```
config switch-controller storm-control
    Description: Configure FortiSwitch storm control.
    set broadcast [enable|disable]
    set rate {integer}
    set unknown-multicast [enable|disable]
    set unknown-unicast [enable|disable]
end
```

## config switch-controller storm-control

Parameter	Description	Type	Size	Default
broadcast	Enable/disable storm control to drop broadcast traffic.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable broadcast storm control.		
	<i>disable</i>	Disable broadcast storm control.		
rate	Rate in packets per second at which storm traffic is controlled. Storm control drops excess traffic data rates beyond this threshold.	integer	Minimum value: 1 Maximum value: 10000000	500
unknown-multicast	Enable/disable storm control to drop unknown multicast traffic.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable unknown multicast storm control.		
	<i>disable</i>	Disable unknown multicast storm control.		
unknown-unicast	Enable/disable storm control to drop unknown unicast traffic.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable unknown unicast storm control.		
	<i>disable</i>	Disable unknown unicast storm control.		

## config switch-controller stp-instance



This command is available for model(s): FortiGate 1000D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001E1, FortiGate 5001E.

Configure FortiSwitch multiple spanning tree protocol (MSTP) instances.

```
config switch-controller stp-instance
    Description: Configure FortiSwitch multiple spanning tree protocol (MSTP) instances.
    edit <id>
        set vlan-range <vlan-name1>, <vlan-name2>, ...
    next
end
```

## config switch-controller stp-instance

Parameter	Description	Type	Size	Default
id	Instance ID.	string	Maximum length: 2	
vlan-range <vlan-name>	Configure VLAN range for STP instance. VLAN name.	string	Maximum length: 79	

## config switch-controller stp-settings



This command is available for model(s): FortiGate 1000D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001E1, FortiGate 5001E.

Configure FortiSwitch spanning tree protocol (STP).

```
config switch-controller stp-settings
    Description: Configure FortiSwitch spanning tree protocol (STP).
    set forward-time {integer}
    set hello-time {integer}
    set max-age {integer}
    set max-hops {integer}
    set name {string}
    set pending-timer {integer}
    set revision {integer}
end
```

## config switch-controller stp-settings

Parameter	Description	Type	Size	Default
forward-time	Period of time a port is in listening and learning state.	integer	Minimum value: 4 Maximum value: 30	15

Parameter	Description	Type	Size	Default
hello-time	Period of time between successive STP frame Bridge Protocol Data Units.	integer	Minimum value: 1 Maximum value: 10	2
max-age	Maximum time before a bridge port expires its configuration BPDU information.	integer	Minimum value: 6 Maximum value: 40	20
max-hops	Maximum number of hops between the root bridge and the furthest bridge.	integer	Minimum value: 1 Maximum value: 40	20
name	Name of global STP settings configuration.	string	Maximum length: 31	
pending-timer	Pending time.	integer	Minimum value: 1 Maximum value: 15	4
revision	STP revision number.	integer	Minimum value: 0 Maximum value: 65535	0



## config switch-controller switch-group



This command is available for model(s): FortiGate 1000D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001E1, FortiGate 5001E.

Configure FortiSwitch switch groups.

```
config switch-controller switch-group
    Description: Configure FortiSwitch switch groups.
    edit <name>
        set description {string}
        set fortilink {string}
        set members <switch-id1>, <switch-id2>, ...
    next
end
```

## config switch-controller switch-group

Parameter	Description	Type	Size	Default
description	Optional switch group description.	string	Maximum length: 63	
fortilink	FortiLink interface to which switch group members belong.	string	Maximum length: 15	
members <switch-id>	FortiSwitch members belonging to this switch group. Managed device ID.	string	Maximum length: 79	

Parameter	Description	Type	Size	Default
name	Switch group name.	string	Maximum length: 35	

## config switch-controller switch-interface-tag



This command is available for model(s): FortiGate 1000D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001E1, FortiGate 5001E.

Configure switch object tags.

```
config switch-controller switch-interface-tag
    Description: Configure switch object tags.
    edit <name>
    next
end
```

## config switch-controller switch-interface-tag

Parameter	Description	Type	Size	Default
name	Tag name.	string	Maximum length: 63	

## config switch-controller switch-log



This command is available for model(s): FortiGate 1000D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001E1, FortiGate 5001E.

Configure FortiSwitch logging (logs are transferred to and inserted into FortiGate event log).

```
config switch-controller switch-log
    Description: Configure FortiSwitch logging (logs are transferred to and inserted into
FortiGate event log).
    set severity [emergency|alert|...]
    set status [enable|disable]
end
```

## config switch-controller switch-log

Parameter	Description	Type	Size	Default								
severity	Severity of FortiSwitch logs that are added to the FortiGate event log.	option	-	notification								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>emergency</i></td><td>Emergency level.</td></tr><tr><td><i>alert</i></td><td>Alert level.</td></tr><tr><td><i>critical</i></td><td>Critical level.</td></tr></table>	Option	Description	<i>emergency</i>	Emergency level.	<i>alert</i>	Alert level.	<i>critical</i>	Critical level.			
Option	Description											
<i>emergency</i>	Emergency level.											
<i>alert</i>	Alert level.											
<i>critical</i>	Critical level.											

Parameter	Description	Type	Size	Default												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>error</i></td><td>Error level.</td></tr><tr><td><i>warning</i></td><td>Warning level.</td></tr><tr><td><i>notification</i></td><td>Notification level.</td></tr><tr><td><i>information</i></td><td>Information level.</td></tr><tr><td><i>debug</i></td><td>Debug level.</td></tr></table>	Option	Description	<i>error</i>	Error level.	<i>warning</i>	Warning level.	<i>notification</i>	Notification level.	<i>information</i>	Information level.	<i>debug</i>	Debug level.			
	Option	Description														
	<i>error</i>	Error level.														
	<i>warning</i>	Warning level.														
	<i>notification</i>	Notification level.														
	<i>information</i>	Information level.														
<i>debug</i>	Debug level.															
status	Enable/disable adding FortiSwitch logs to FortiGate event log.	option	-	enable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Add FortiSwitch logs to FortiGate event log.</td></tr><tr><td><i>disable</i></td><td>Do not add FortiSwitch logs to FortiGate event log.</td></tr></table>	Option	Description	<i>enable</i>	Add FortiSwitch logs to FortiGate event log.	<i>disable</i>	Do not add FortiSwitch logs to FortiGate event log.									
	Option	Description														
	<i>enable</i>	Add FortiSwitch logs to FortiGate event log.														
<i>disable</i>	Do not add FortiSwitch logs to FortiGate event log.															

## config switch-controller switch-profile



This command is available for model(s): FortiGate 1000D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001E1, FortiGate 5001E.

Configure FortiSwitch switch profile.

```

config switch-controller switch-profile
    Description: Configure FortiSwitch switch profile.
    edit <name>
        set login-passwd {password}
        set login-passwd-override [enable|disable]
    next
end

```

## config switch-controller switch-profile

Parameter	Description	Type	Size	Default						
login-passwd	Login password of managed FortiSwitch.	password	Not Specified							
login-passwd-override	Enable/disable overriding the admin administrator password for a managed FortiSwitch with the FortiGate admin administrator account password.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Override a managed FortiSwitch's admin administrator password.</td></tr><tr><td><i>disable</i></td><td>Use the managed FortiSwitch admin administrator account password.</td></tr></table>				Option	Description	<i>enable</i>	Override a managed FortiSwitch's admin administrator password.	<i>disable</i>	Use the managed FortiSwitch admin administrator account password.
Option	Description									
<i>enable</i>	Override a managed FortiSwitch's admin administrator password.									
<i>disable</i>	Use the managed FortiSwitch admin administrator account password.									
name	FortiSwitch Profile name.	string	Maximum length: 35							

## config switch-controller system



This command is available for model(s): FortiGate 1000D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001E1, FortiGate 5001E.

Configure system-wide switch controller settings.

```
config switch-controller system
    Description: Configure system-wide switch controller settings.
    set data-sync-interval {integer}
    set dynamic-periodic-interval {integer}
    set iot-holdoff {integer}
    set iot-mac-idle {integer}
    set iot-scan-interval {integer}
    set iot-weight-threshold {integer}
    set nac-periodic-interval {integer}
    set parallel-process {integer}
    set parallel-process-override [disable|enable]
    set tunnel-mode [compatible|strict]
end
```

## config switch-controller system

Parameter	Description	Type	Size	Default
data-sync-interval	Time interval between collection of switch data.	integer	Minimum value: 30 Maximum value: 1800	60

Parameter	Description	Type	Size	Default
dynamic-periodic-interval	Periodic time interval to run Dynamic port policy engine.	integer	Minimum value: 5 Maximum value: 60	15
iot-holdoff	MAC entry's creation time. Time must be greater than this value for an entry to be created.	integer	Minimum value: 0 Maximum value: 10080	5
iot-mac-idle	MAC entry's idle time. MAC entry is removed after this value.	integer	Minimum value: 0 Maximum value: 10080	1440
iot-scan-interval	IoT scan interval.	integer	Minimum value: 2 Maximum value: 10080	60
iot-weight-threshold	MAC entry's confidence value. Value is re-queried when below this value.	integer	Minimum value: 0 Maximum value: 255	1
nac-periodic-interval	Periodic time interval to run NAC engine.	integer	Minimum value: 5 Maximum value: 60	15
parallel-process	Maximum number of parallel processes.	integer	Minimum value: 1 Maximum value: 128 **	1
parallel-process-override	Enable/disable parallel process override.	option	-	disable
	Option	Description		
	disable	Disable maximum parallel process override.		
	enable	Enable maximum parallel process override.		
tunnel-mode	Compatible/strict tunnel mode.	option	-	compatible

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>compatible</i>	Allow for backward compatible ciphers.		
	<i>strict</i>	Follow system.strong-crypto ciphers.		

\*\* Values may differ between models.

## config switch-controller traffic-policy



This command is available for model(s): FortiGate 1000D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001E1, FortiGate 5001E.

Configure FortiSwitch traffic policy.

```
config switch-controller traffic-policy
  Description: Configure FortiSwitch traffic policy.
  edit <name>
    set cos-queue {integer}
    set description {string}
    set guaranteed-bandwidth {integer}
    set guaranteed-burst {integer}
    set maximum-burst {integer}
    set policer-status [enable|disable]
    set type [ingress|egress]
  next
end
```



## config switch-controller traffic-policy

Parameter	Description	Type	Size	Default						
cos-queue	COS queue, or unset to disable.	integer	Minimum value: 0 Maximum value: 7							
description	Description of the traffic policy.	string	Maximum length: 63							
guaranteed-bandwidth	Guaranteed bandwidth in kbps (max value = 524287000).	integer	Minimum value: 0 Maximum value: 524287000	10000						
guaranteed-burst	Guaranteed burst size in bytes (max value = 4294967295).	integer	Minimum value: 0 Maximum value: 4294967295	45000						
maximum-burst	Maximum burst size in bytes (max value = 4294967295).	integer	Minimum value: 0 Maximum value: 4294967295	67500						
name	Traffic policy name.	string	Maximum length: 63							
policer-status	Enable/disable policer config on the traffic policy.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable policer config on the traffic policy.</td></tr><tr><td>disable</td><td>Disable policer config on the traffic policy.</td></tr></table>				Option	Description	enable	Enable policer config on the traffic policy.	disable	Disable policer config on the traffic policy.
Option	Description									
enable	Enable policer config on the traffic policy.									
disable	Disable policer config on the traffic policy.									
type	Configure type of policy(ingress/egress).	option	-	ingress						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ingress</td><td>Ingress policy.</td></tr><tr><td>egress</td><td>Egress policy.</td></tr></table>				Option	Description	ingress	Ingress policy.	egress	Egress policy.
Option	Description									
ingress	Ingress policy.									
egress	Egress policy.									

---

## config switch-controller traffic-sniffer

---



This command is available for model(s): FortiGate 1000D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001E1, FortiGate 5001E.

---

Configure FortiSwitch RSPAN/ERSPAN traffic sniffing parameters.

```
config switch-controller traffic-sniffer
  Description: Configure FortiSwitch RSPAN/ERSPAN traffic sniffing parameters.
  set erspan-ip {ipv4-address}
  set mode [erspan-auto|rspan|...]
  config target-ip
    Description: Sniffer IPs to filter.
    edit <ip>
      set description {string}
    next
  end
  config target-mac
    Description: Sniffer MACs to filter.
    edit <mac>
      set description {string}
    next
  end
  config target-port
    Description: Sniffer ports to filter.
    edit <switch-id>
      set description {string}
      set in-ports <name1>, <name2>, ...
      set out-ports <name1>, <name2>, ...
    next
  end
end
```

## config switch-controller traffic-sniffer

Parameter	Description	Type	Size	Default
erspan-ip	Configure ERSPAN collector IP address.	ipv4-address	Not Specified	0.0.0.0
mode	Configure traffic sniffer mode.	option	-	erspan-auto
	Option	Description		
	<i>erspan-auto</i>	Mirror traffic using a GRE tunnel.		
	<i>rspan</i>	Mirror traffic on a layer2 VLAN.		
	<i>none</i>	Disable traffic mirroring (sniffer).		

## config target-ip

Parameter	Description	Type	Size	Default
ip	Sniffer IP.	ipv4-address	Not Specified	0.0.0.0
description	Description for the sniffer IP.	string	Maximum length: 63	

## config target-mac

Parameter	Description	Type	Size	Default
mac	Sniffer MAC.	mac-address	Not Specified	00:00:00:00:00:00
description	Description for the sniffer MAC.	string	Maximum length: 63	

## config target-port

Parameter	Description	Type	Size	Default
switch-id	Managed-switch ID.	string	Maximum length: 16	
description	Description for the sniffer port entry.	string	Maximum length: 63	
in-ports <name>	Configure source ingress port interfaces. Interface name.	string	Maximum length: 79	
out-ports <name>	Configure source egress port interfaces. Interface name.	string	Maximum length: 79	

## config switch-controller virtual-port-pool



This command is available for model(s): FortiGate 1000D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001E1, FortiGate 5001E.

Configure virtual pool.

```
config switch-controller virtual-port-pool
    Description: Configure virtual pool.
    edit <name>
        set description {string}
    next
end
```

## config switch-controller virtual-port-pool

Parameter	Description	Type	Size	Default
description	Virtual switch pool description.	string	Maximum length: 63	
name	Virtual switch pool name.	string	Maximum length: 35	

## config switch-controller vlan-policy



This command is available for model(s): FortiGate 1000D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 5001E1, FortiGate 5001E.

Configure VLAN policy to be applied on the managed FortiSwitch ports through dynamic-port-policy.

```
config switch-controller vlan-policy
    Description: Configure VLAN policy to be applied on the managed FortiSwitch ports
    through dynamic-port-policy.
    edit <name>
        set allowed-vlans <vlan-name1>, <vlan-name2>, ...
        set allowed-vlans-all [enable|disable]
        set description {string}
        set discard-mode [none|all-untagged|...]
        set fortilink {string}
        set untagged-vlans <vlan-name1>, <vlan-name2>, ...
        set vlan {string}
    next
end
```

## config switch-controller vlan-policy

Parameter	Description	Type	Size	Default
allowed-vlans <vlan-name>	Allowed VLANs to be applied when using this VLAN policy. VLAN name.	string	Maximum length: 79	

Parameter	Description	Type	Size	Default
allowed-vlans-all	Enable/disable all defined VLANs when using this VLAN policy.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable all defined VLANs.		
	<i>disable</i>	Disable all defined VLANs.		
description	Description for the VLAN policy.	string	Maximum length: 63	
discard-mode	Discard mode to be applied when using this VLAN policy.	option	-	none
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	Discard disabled.		
	<i>all-untagged</i>	Discard all frames that are untagged.		
	<i>all-tagged</i>	Discard all frames that are tagged.		
fortilink	FortiLink interface for which this VLAN policy belongs to.	string	Maximum length: 15	
name	VLAN policy name.	string	Maximum length: 63	
untagged-vlans <vlan-name>	Untagged VLANs to be applied when using this VLAN policy. VLAN name.	string	Maximum length: 79	
vlan	Native VLAN to be applied when using this VLAN policy.	string	Maximum length: 15	

# system

This section includes syntax for the following commands:

- [config system 3g-modem custom on page 1030](#)
- [config system accprofile on page 1031](#)
- [config system acme on page 1041](#)
- [config system admin on page 1042](#)
- [config system affinity-interrupt on page 1049](#)
- [config system affinity-packet-redistribution on page 1050](#)
- [config system alarm on page 1051](#)
- [config system alias on page 1054](#)
- [config system api-user on page 1055](#)
- [config system arp-table on page 1056](#)
- [config system auto-install on page 1057](#)
- [config system auto-script on page 1058](#)
- [config system automation-action on page 1059](#)
- [config system automation-destination on page 1064](#)
- [config system automation-stitch on page 1064](#)
- [config system automation-trigger on page 1066](#)
- [config system autoupdate schedule on page 1070](#)
- [config system autoupdate tunneling on page 1071](#)
- [config system bypass on page 1072](#)
- [config system central-management on page 1073](#)
- [config system cluster-sync on page 1078](#)
- [config system console on page 1081](#)
- [config system csf on page 1082](#)
- [config system custom-language on page 1087](#)
- [config system ddns on page 1088](#)
- [config system dedicated-mgmt on page 1090](#)
- [config system dhcp6 server on page 1091](#)
- [config system dhcp server on page 1095](#)
- [config system dnp3-proxy on page 1107](#)
- [config system dns-database on page 1109](#)
- [config system dns-server on page 1112](#)
- [config system dns on page 1113](#)
- [config system dns64 on page 1116](#)
- [config system dscp-based-priority on page 1116](#)
- [config system elbc on page 1117](#)
- [config system email-server on page 1118](#)
- [config system external-resource on page 1120](#)

- 
- [config system federated-upgrade on page 1123](#)
  - [config system fips-cc on page 1125](#)
  - [config system fortiguard on page 1126](#)
  - [config system fortindr on page 1134](#)
  - [config system fortisandbox on page 1135](#)
  - [config system fsso-polling on page 1137](#)
  - [config system ftm-push on page 1138](#)
  - [config system geneve on page 1138](#)
  - [config system geoip-override on page 1139](#)
  - [config system gi-gk on page 1141](#)
  - [config system global on page 1142](#)
  - [config system gre-tunnel on page 1193](#)
  - [config system ha-monitor on page 1196](#)
  - [config system ha on page 1197](#)
  - [config system ike on page 1210](#)
  - [config system interface on page 1223](#)
  - [config system ipam on page 1282](#)
  - [config system ipip-tunnel on page 1283](#)
  - [config system ips-urlfilter-dns on page 1284](#)
  - [config system ips-urlfilter-dns6 on page 1285](#)
  - [config system ips on page 1285](#)
  - [config system ipsec-aggregate on page 1286](#)
  - [config system ipv6-neighbor-cache on page 1287](#)
  - [config system ipv6-tunnel on page 1287](#)
  - [config system isf-queue-profile on page 1289](#)
  - [config system link-monitor on page 1291](#)
  - [config system lldp network-policy on page 1296](#)
  - [config system lte-modem on page 1304](#)
  - [config system mac-address-table on page 1309](#)
  - [config system management-tunnel on page 1309](#)
  - [config system mobile-tunnel on page 1311](#)
  - [config system modem on page 1314](#)
  - [config system nd-proxy on page 1321](#)
  - [config system netflow on page 1322](#)
  - [config system network-visibility on page 1323](#)
  - [config system np6 on page 1325](#)
  - [config system np6xlite on page 1337](#)
  - [config system npu-setting prp on page 1350](#)
  - [config system npu-vlink on page 1351](#)
  - [config system npu on page 1352](#)
  - [config system ntp on page 1411](#)
  - [config system object-tagging on page 1414](#)
  - [config system password-policy-guest-admin on page 1415](#)



- 
- [config system password-policy on page 1417](#)
  - [config system physical-switch on page 1419](#)
  - [config system pppoe-interface on page 1420](#)
  - [config system probe-response on page 1422](#)
  - [config system proxy-arp on page 1424](#)
  - [config system ptp on page 1424](#)
  - [config system replacemsg-group on page 1426](#)
  - [config system replacemsg-image on page 1438](#)
  - [config system replacemsg admin on page 1439](#)
  - [config system replacemsg alertmail on page 1440](#)
  - [config system replacemsg auth on page 1441](#)
  - [config system replacemsg automation on page 1442](#)
  - [config system replacemsg custom-message on page 1443](#)
  - [config system replacemsg fortiguard-wf on page 1443](#)
  - [config system replacemsg ftp on page 1444](#)
  - [config system replacemsg http on page 1445](#)
  - [config system replacemsg icap on page 1446](#)
  - [config system replacemsg mail on page 1447](#)
  - [config system replacemsg nac-quar on page 1448](#)
  - [config system replacemsg spam on page 1449](#)
  - [config system replacemsg sslvpn on page 1449](#)
  - [config system replacemsg traffic-quota on page 1450](#)
  - [config system replacemsg utm on page 1451](#)
  - [config system replacemsg webproxy on page 1452](#)
  - [config system resource-limits on page 1453](#)
  - [config system saml on page 1456](#)
  - [config system sdn-connector on page 1459](#)
  - [config system sdwan on page 1468](#)
  - [config system session-helper on page 1488](#)
  - [config system session-ttl on page 1490](#)
  - [config system settings on page 1491](#)
  - [config system sflow on page 1513](#)
  - [config system sit-tunnel on page 1514](#)
  - [config system smc-ntp on page 1516](#)
  - [config system sms-server on page 1517](#)
  - [config system snmp community on page 1518](#)
  - [config system snmp sysinfo on page 1525](#)
  - [config system snmp user on page 1527](#)
  - [config system speed-test-schedule on page 1533](#)
  - [config system speed-test-server on page 1535](#)
  - [config system sso-admin on page 1536](#)
  - [config system sso-forticloud-admin on page 1537](#)
  - [config system standalone-cluster on page 1537](#)

- [config system storage on page 1538](#)
- [config system stp on page 1540](#)
- [config system switch-interface on page 1542](#)
- [config system tos-based-priority on page 1544](#)
- [config system vdom-dns on page 1545](#)
- [config system vdom-exception on page 1546](#)
- [config system vdom-link on page 1548](#)
- [config system vdom-netflow on page 1549](#)
- [config system vdom-property on page 1550](#)
- [config system vdom-radius-server on page 1552](#)
- [config system vdom-sflow on page 1552](#)
- [config system vdom on page 1553](#)
- [config system virtual-switch on page 1555](#)
- [config system virtual-wire-pair on page 1557](#)
- [config system vne-tunnel on page 1558](#)
- [config system vxlan on page 1559](#)
- [config system wccp on page 1560](#)
- [config system wireless ap-status on page 1564](#)
- [config system wireless settings on page 1565](#)
- [config system zone on page 1568](#)

## config system 3g-modem custom



This command is available for model(s): FortiGate 1000D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate VM64.

### 3G MODEM custom.

```
config system 3g-modem custom
  Description: 3G MODEM custom.
  edit <id>
    set class-id {user}
    set init-string {string}
    set model {string}
    set modeswitch-string {string}
    set product-id {user}
    set vendor {string}
    set vendor-id {user}
  next
end
```

### config system 3g-modem custom

Parameter	Description	Type	Size	Default
class-id	USB interface class in hexadecimal format (00-ff).	user	Not Specified	
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
init-string	Init string in hexadecimal format (even length).	string	Maximum length: 127	
model	MODEM model name.	string	Maximum length: 35	
modeswitch-string	USB modeswitch arguments. e.g: '-v 1410 -p 9030 -V 1410 -P 9032 -u 3'	string	Maximum length: 127	
product-id	USB product ID in hexadecimal format (0000-ffff).	user	Not Specified	
vendor	MODEM vendor name.	string	Maximum length: 35	
vendor-id	USB vendor ID in hexadecimal format (0000-ffff).	user	Not Specified	

### config system accprofile

Configure access profiles for system administrators.

```
config system accprofile
  Description: Configure access profiles for system administrators.
  edit <name>
    set admintimeout {integer}
    set admintimeout-override [enable|disable]
    set authgrp [none|read|...]
    set comments {var-string}
```

```
set ftviewgrp [none|read|...]
set fwgrp [none|read|...]
config fwgrp-permission
    Description: Custom firewall permission.
    set policy [none|read|...]
    set address [none|read|...]
    set service [none|read|...]
    set schedule [none|read|...]
    set others [none|read|...]
end
set loggrp [none|read|...]
config loggrp-permission
    Description: Custom Log & Report permission.
    set config [none|read|...]
    set data-access [none|read|...]
    set report-access [none|read|...]
    set threat-weight [none|read|...]
end
set netgrp [none|read|...]
config netgrp-permission
    Description: Custom network permission.
    set cfg [none|read|...]
    set packet-capture [none|read|...]
    set route-cfg [none|read|...]
end
set scope [vdom|global]
set secfabgrp [none|read|...]
set sysgrp [none|read|...]
config sysgrp-permission
    Description: Custom system permission.
    set admin [none|read|...]
    set upd [none|read|...]
    set cfg [none|read|...]
    set mnt [none|read|...]
end
set system-diagnostics [enable|disable]
set utmgrp [none|read|...]
config utmgrp-permission
    Description: Custom Security Profile permissions.
    set antivirus [none|read|...]
    set ips [none|read|...]
    set webfilter [none|read|...]
    set emailfilter [none|read|...]
    set data-loss-prevention [none|read|...]
    set file-filter [none|read|...]
    set application-control [none|read|...]
    set icap [none|read|...]
    set voip [none|read|...]
    set waf [none|read|...]
    set dnsfilter [none|read|...]
    set endpoint-control [none|read|...]
end
set vpngrp [none|read|...]
set wanoptgrp [none|read|...]
set wifi [none|read|...]
next
```

end

## config system accprofile

Parameter	Description	Type	Size	Default
admintimeout	Administrator timeout for this access profile.	integer	Minimum value: 1 Maximum value: 480	10
admintimeout-override	Enable/disable overriding the global administrator idle timeout.	option	-	disable
	Option	Description		
	enable	Enable overriding the global administrator idle timeout.		
	disable	Disable overriding the global administrator idle timeout.		
authgrp	Administrator access to Users and Devices.	option	-	none
	Option	Description		
	none	No access.		
	read	Read access.		
	read-write	Read/write access.		
comments	Comment.	var-string	Maximum length: 255	
ftviewgrp	FortiView.	option	-	none
	Option	Description		
	none	No access.		
	read	Read access.		
	read-write	Read/write access.		
fwgrp	Administrator access to the Firewall configuration.	option	-	none
	Option	Description		
	none	No access.		
	read	Read access.		
	read-write	Read/write access.		
	custom	Customized access.		

Parameter	Description	Type	Size	Default
loggrp	Administrator access to Logging and Reporting including viewing log messages.	option	-	none
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		
	<i>custom</i>	Customized access.		
name	Profile name.	string	Maximum length: 35	
netgrp	Network Configuration.	option	-	none
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		
	<i>custom</i>	Customized access.		
scope	Scope of admin access: global or specific VDOM(s).	option	-	vdom
	<b>Option</b>	<b>Description</b>		
	<i>vdom</i>	VDOM access.		
	<i>global</i>	Global access.		
secfabgrp	Security Fabric.	option	-	none
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		
sysgrp	System Configuration.	option	-	none
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>read-write</i>	Read/write access.		
	<i>custom</i>	Customized access.		
system-diagnostics	Enable/disable permission to run system diagnostic commands.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable permission to run system diagnostic commands.		
	<i>disable</i>	Disable permission to run system diagnostic commands.		
utmgrp	Administrator access to Security Profiles.	option	-	none
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		
	<i>custom</i>	Customized access.		
vpngrp	Administrator access to IPsec, SSL, PPTP, and L2TP VPN.	option	-	none
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		
wanoptgrp *	Administrator access to WAN Opt & Cache.	option	-	none
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		
wifi	Administrator access to the WiFi controller and Switch controller.	option	-	none

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		

\* This parameter may not exist in some models.

### config fwgrp-permission

Parameter	Description	Type	Size	Default
policy	Policy Configuration.	option	-	none
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		
address	Address Configuration.	option	-	none
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		
service	Service Configuration.	option	-	none
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		
schedule	Schedule Configuration.	option	-	none
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		



Parameter	Description	Type	Size	Default
others	Other Firewall Configuration.	option	-	none
	Option	Description		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		

### config loggrp-permission

Parameter	Description	Type	Size	Default								
config	Log & Report configuration.	option	-	none								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>No access.</td></tr><tr><td><i>read</i></td><td>Read access.</td></tr><tr><td><i>read-write</i></td><td>Read/write access.</td></tr></table>	Option	Description	<i>none</i>	No access.	<i>read</i>	Read access.	<i>read-write</i>	Read/write access.			
Option	Description											
<i>none</i>	No access.											
<i>read</i>	Read access.											
<i>read-write</i>	Read/write access.											
data-access	Log & Report Data Access.	option	-	none								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>No access.</td></tr><tr><td><i>read</i></td><td>Read access.</td></tr><tr><td><i>read-write</i></td><td>Read/write access.</td></tr></table>	Option	Description	<i>none</i>	No access.	<i>read</i>	Read access.	<i>read-write</i>	Read/write access.			
Option	Description											
<i>none</i>	No access.											
<i>read</i>	Read access.											
<i>read-write</i>	Read/write access.											
report-access	Log & Report Report Access.	option	-	none								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>No access.</td></tr><tr><td><i>read</i></td><td>Read access.</td></tr><tr><td><i>read-write</i></td><td>Read/write access.</td></tr></table>	Option	Description	<i>none</i>	No access.	<i>read</i>	Read access.	<i>read-write</i>	Read/write access.			
Option	Description											
<i>none</i>	No access.											
<i>read</i>	Read access.											
<i>read-write</i>	Read/write access.											
threat-weight	Log & Report Threat Weight.	option	-	none								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>No access.</td></tr><tr><td><i>read</i></td><td>Read access.</td></tr><tr><td><i>read-write</i></td><td>Read/write access.</td></tr></table>	Option	Description	<i>none</i>	No access.	<i>read</i>	Read access.	<i>read-write</i>	Read/write access.			
Option	Description											
<i>none</i>	No access.											
<i>read</i>	Read access.											
<i>read-write</i>	Read/write access.											

## config netgrp-permission

Parameter	Description	Type	Size	Default
cfg	Network Configuration.	option	-	none
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		
packet-capture	Packet Capture Configuration.	option	-	none
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		
route-cfg	Router Configuration.	option	-	none
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		

## config sysgrp-permission

Parameter	Description	Type	Size	Default
admin	Administrator Users.	option	-	none
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		
upd	FortiGuard Updates.	option	-	none
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		

Parameter	Description	Type	Size	Default
cfg	System Configuration.	option	-	none
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		
mnt	Maintenance.	option	-	none
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		

### config utmgrp-permission

Parameter	Description	Type	Size	Default
antivirus	Antivirus profiles and settings.	option	-	none
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		
ips	IPS profiles and settings.	option	-	none
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		
webfilter	Web Filter profiles and settings.	option	-	none
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		

Parameter	Description	Type	Size	Default								
emailfilter	Email Filter and settings.	option	-	none								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>No access.</td></tr><tr><td><i>read</i></td><td>Read access.</td></tr><tr><td><i>read-write</i></td><td>Read/write access.</td></tr></table>	Option	Description	<i>none</i>	No access.	<i>read</i>	Read access.	<i>read-write</i>	Read/write access.			
Option	Description											
<i>none</i>	No access.											
<i>read</i>	Read access.											
<i>read-write</i>	Read/write access.											
data-loss-prevention	DLP profiles and settings.	option	-	none								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>No access.</td></tr><tr><td><i>read</i></td><td>Read access.</td></tr><tr><td><i>read-write</i></td><td>Read/write access.</td></tr></table>	Option	Description	<i>none</i>	No access.	<i>read</i>	Read access.	<i>read-write</i>	Read/write access.			
Option	Description											
<i>none</i>	No access.											
<i>read</i>	Read access.											
<i>read-write</i>	Read/write access.											
file-filter	File-filter profiles and settings.	option	-	none								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>No access.</td></tr><tr><td><i>read</i></td><td>Read access.</td></tr><tr><td><i>read-write</i></td><td>Read/write access.</td></tr></table>	Option	Description	<i>none</i>	No access.	<i>read</i>	Read access.	<i>read-write</i>	Read/write access.			
Option	Description											
<i>none</i>	No access.											
<i>read</i>	Read access.											
<i>read-write</i>	Read/write access.											
application-control	Application Control profiles and settings.	option	-	none								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>No access.</td></tr><tr><td><i>read</i></td><td>Read access.</td></tr><tr><td><i>read-write</i></td><td>Read/write access.</td></tr></table>	Option	Description	<i>none</i>	No access.	<i>read</i>	Read access.	<i>read-write</i>	Read/write access.			
Option	Description											
<i>none</i>	No access.											
<i>read</i>	Read access.											
<i>read-write</i>	Read/write access.											
icap	ICAP profiles and settings.	option	-	none								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>No access.</td></tr><tr><td><i>read</i></td><td>Read access.</td></tr><tr><td><i>read-write</i></td><td>Read/write access.</td></tr></table>	Option	Description	<i>none</i>	No access.	<i>read</i>	Read access.	<i>read-write</i>	Read/write access.			
Option	Description											
<i>none</i>	No access.											
<i>read</i>	Read access.											
<i>read-write</i>	Read/write access.											
voip	VoIP profiles and settings.	option	-	none								

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		
waf	Web Application Firewall profiles and settings.	option	-	none
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		
dnsfilter	DNS Filter profiles and settings.	option	-	none
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		
endpoint-control	FortiClient Profiles.	option	-	none
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	No access.		
	<i>read</i>	Read access.		
	<i>read-write</i>	Read/write access.		

## config system acme

Configure ACME client.

```

config system acme
  Description: Configure ACME client.
  config accounts
    Description: ACME accounts list.
    edit <id>
      set status {string}
      set url {string}
      set ca_url {string}
      set email {string}
      set privatekey {string}
    next
  
```

```

end
set interface <interface-name1>, <interface-name2>, ...
set source-ip {ipv4-address}
set source-ip6 {ipv6-address}
end

```

## config system acme

Parameter	Description	Type	Size	Default
interface <interface-name>	Interface(s) on which the ACME client will listen for challenges. Interface name.	string	Maximum length: 79	
source-ip	Source IPv4 address used to connect to the ACME server.	ipv4-address	Not Specified	0.0.0.0
source-ip6	Source IPv6 address used to connect to the ACME server.	ipv6-address	Not Specified	::

## config accounts

Parameter	Description	Type	Size	Default
id	Account id.	string	Maximum length: 255	
status	Account status.	string	Maximum length: 127	
url	Account url.	string	Maximum length: 511	
ca_url	Account ca_url.	string	Maximum length: 255	
email	Account email.	string	Maximum length: 255	
privatekey	Account Private Key.	string	Maximum length: 8191	

## config system admin

Configure admin users.

```

config system admin
  Description: Configure admin users.
  edit <name>
    set accprofile {string}
    set accprofile-override [enable|disable]
    set allow-remove-admin-session [enable|disable]
    set comments {var-string}
  end
end

```

```
set email-to {string}
set force-password-change [enable|disable]
set fortitoken {string}
set guest-auth [disable|enable]
set guest-lang {string}
set guest-usergroups <name1>, <name2>, ...
set ip6-trusthost1 {ipv6-prefix}
set ip6-trusthost10 {ipv6-prefix}
set ip6-trusthost2 {ipv6-prefix}
set ip6-trusthost3 {ipv6-prefix}
set ip6-trusthost4 {ipv6-prefix}
set ip6-trusthost5 {ipv6-prefix}
set ip6-trusthost6 {ipv6-prefix}
set ip6-trusthost7 {ipv6-prefix}
set ip6-trusthost8 {ipv6-prefix}
set ip6-trusthost9 {ipv6-prefix}
set password {password-2}
set password-expire {user}
set peer-auth [enable|disable]
set peer-group {string}
set radius-vdom-override [enable|disable]
set remote-auth [enable|disable]
set remote-group {string}
set schedule {string}
set sms-custom-server {string}
set sms-phone {string}
set sms-server [fortiguard|custom]
set ssh-certificate {string}
set ssh-public-key1 {user}
set ssh-public-key2 {user}
set ssh-public-key3 {user}
set trusthost1 {ipv4-classnet}
set trusthost10 {ipv4-classnet}
set trusthost2 {ipv4-classnet}
set trusthost3 {ipv4-classnet}
set trusthost4 {ipv4-classnet}
set trusthost5 {ipv4-classnet}
set trusthost6 {ipv4-classnet}
set trusthost7 {ipv4-classnet}
set trusthost8 {ipv4-classnet}
set trusthost9 {ipv4-classnet}
set two-factor [disable|fortitoken|...]
set two-factor-authentication [fortitoken|email|...]
set two-factor-notification [email|sms]
set vdom <name1>, <name2>, ...
set wildcard [enable|disable]
next
end
```

## config system admin

Parameter	Description	Type	Size	Default						
accprofile	Access profile for this administrator. Access profiles control administrator access to FortiGate features.	string	Maximum length: 35							
accprofile-override	Enable to use the name of an access profile provided by the remote authentication server to control the FortiGate features that this administrator can access.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable access profile override.</td></tr><tr><td><i>disable</i></td><td>Disable access profile override.</td></tr></table>	Option	Description	<i>enable</i>	Enable access profile override.	<i>disable</i>	Disable access profile override.			
Option	Description									
<i>enable</i>	Enable access profile override.									
<i>disable</i>	Disable access profile override.									
allow-remove-admin-session	Enable/disable allow admin session to be removed by privileged admin users.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable allow-remove option.</td></tr><tr><td><i>disable</i></td><td>Disable allow-remove option.</td></tr></table>	Option	Description	<i>enable</i>	Enable allow-remove option.	<i>disable</i>	Disable allow-remove option.			
Option	Description									
<i>enable</i>	Enable allow-remove option.									
<i>disable</i>	Disable allow-remove option.									
comments	Comment.	var-string	Maximum length: 255							
email-to	This administrator's email address.	string	Maximum length: 63							
force-password-change	Enable/disable force password change on next login.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable force password change on next login.</td></tr><tr><td><i>disable</i></td><td>Disable force password change on next login.</td></tr></table>	Option	Description	<i>enable</i>	Enable force password change on next login.	<i>disable</i>	Disable force password change on next login.			
Option	Description									
<i>enable</i>	Enable force password change on next login.									
<i>disable</i>	Disable force password change on next login.									
fortitoken	This administrator's FortiToken serial number.	string	Maximum length: 16							
guest-auth	Enable/disable guest authentication.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable guest authentication.</td></tr><tr><td><i>enable</i></td><td>Enable guest authentication.</td></tr></table>	Option	Description	<i>disable</i>	Disable guest authentication.	<i>enable</i>	Enable guest authentication.			
Option	Description									
<i>disable</i>	Disable guest authentication.									
<i>enable</i>	Enable guest authentication.									
guest-lang	Guest management portal language.	string	Maximum length: 35							



Parameter	Description	Type	Size	Default
guest-usergroups <name>	Select guest user groups. Select guest user groups.	string	Maximum length: 79	
ip6-trusthost1	Any IPv6 address from which the administrator can connect to the FortiGate unit. Default allows access from any IPv6 address.	ipv6-prefix	Not Specified	::/0
ip6-trusthost10	Any IPv6 address from which the administrator can connect to the FortiGate unit. Default allows access from any IPv6 address.	ipv6-prefix	Not Specified	::/0
ip6-trusthost2	Any IPv6 address from which the administrator can connect to the FortiGate unit. Default allows access from any IPv6 address.	ipv6-prefix	Not Specified	::/0
ip6-trusthost3	Any IPv6 address from which the administrator can connect to the FortiGate unit. Default allows access from any IPv6 address.	ipv6-prefix	Not Specified	::/0
ip6-trusthost4	Any IPv6 address from which the administrator can connect to the FortiGate unit. Default allows access from any IPv6 address.	ipv6-prefix	Not Specified	::/0
ip6-trusthost5	Any IPv6 address from which the administrator can connect to the FortiGate unit. Default allows access from any IPv6 address.	ipv6-prefix	Not Specified	::/0
ip6-trusthost6	Any IPv6 address from which the administrator can connect to the FortiGate unit. Default allows access from any IPv6 address.	ipv6-prefix	Not Specified	::/0
ip6-trusthost7	Any IPv6 address from which the administrator can connect to the FortiGate unit. Default allows access from any IPv6 address.	ipv6-prefix	Not Specified	::/0
ip6-trusthost8	Any IPv6 address from which the administrator can connect to the FortiGate unit. Default allows access from any IPv6 address.	ipv6-prefix	Not Specified	::/0
ip6-trusthost9	Any IPv6 address from which the administrator can connect to the FortiGate unit. Default allows access from any IPv6 address.	ipv6-prefix	Not Specified	::/0
name	User name.	string	Maximum length: 64	
password	Admin user password.	password-2	Not Specified	
password-expire	Password expire time.	user	Not Specified	

Parameter	Description	Type	Size	Default
peer-auth	Set to enable peer certificate authentication (for HTTPS admin access).	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable peer.		
	<i>disable</i>	Disable peer.		
peer-group	Name of peer group defined under config user group which has PKI members. Used for peer certificate authentication (for HTTPS admin access).	string	Maximum length: 35	
radius-vdom-override	Enable to use the names of VDOMs provided by the remote authentication server to control the VDOMs that this administrator can access.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable VDOM override.		
	<i>disable</i>	Disable VDOM override.		
remote-auth	Enable/disable authentication using a remote RADIUS, LDAP, or TACACS+ server.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable remote authentication.		
	<i>disable</i>	Disable remote authentication.		
remote-group	User group name used for remote auth.	string	Maximum length: 35	
schedule	Firewall schedule used to restrict when the administrator can log in. No schedule means no restrictions.	string	Maximum length: 35	
sms-custom-server	Custom SMS server to send SMS messages to.	string	Maximum length: 35	
sms-phone	Phone number on which the administrator receives SMS messages.	string	Maximum length: 15	
sms-server	Send SMS messages using the FortiGuard SMS server or a custom server.	option	-	fortiguard
	<b>Option</b>	<b>Description</b>		
	<i>fortiguard</i>	Send SMS by FortiGuard.		
	<i>custom</i>	Send SMS by custom server.		

Parameter	Description	Type	Size	Default
ssh-certificate	Select the certificate to be used by the FortiGate for authentication with an SSH client.	string	Maximum length: 35	
ssh-public-key1	Public key of an SSH client. The client is authenticated without being asked for credentials. Create the public-private key pair in the SSH client application.	user	Not Specified	
ssh-public-key2	Public key of an SSH client. The client is authenticated without being asked for credentials. Create the public-private key pair in the SSH client application.	user	Not Specified	
ssh-public-key3	Public key of an SSH client. The client is authenticated without being asked for credentials. Create the public-private key pair in the SSH client application.	user	Not Specified	
trusthost1	Any IPv4 address or subnet address and netmask from which the administrator can connect to the FortiGate unit. Default allows access from any IPv4 address.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0
trusthost10	Any IPv4 address or subnet address and netmask from which the administrator can connect to the FortiGate unit. Default allows access from any IPv4 address.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0
trusthost2	Any IPv4 address or subnet address and netmask from which the administrator can connect to the FortiGate unit. Default allows access from any IPv4 address.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0
trusthost3	Any IPv4 address or subnet address and netmask from which the administrator can connect to the FortiGate unit. Default allows access from any IPv4 address.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0
trusthost4	Any IPv4 address or subnet address and netmask from which the administrator can connect to the FortiGate unit. Default allows access from any IPv4 address.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0
trusthost5	Any IPv4 address or subnet address and netmask from which the administrator can connect to the FortiGate unit. Default allows access from any IPv4 address.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0

Parameter	Description	Type	Size	Default												
trusthost6	Any IPv4 address or subnet address and netmask from which the administrator can connect to the FortiGate unit. Default allows access from any IPv4 address.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0												
trusthost7	Any IPv4 address or subnet address and netmask from which the administrator can connect to the FortiGate unit. Default allows access from any IPv4 address.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0												
trusthost8	Any IPv4 address or subnet address and netmask from which the administrator can connect to the FortiGate unit. Default allows access from any IPv4 address.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0												
trusthost9	Any IPv4 address or subnet address and netmask from which the administrator can connect to the FortiGate unit. Default allows access from any IPv4 address.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0												
two-factor	Enable/disable two-factor authentication.	option	-	disable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable two-factor authentication.</td></tr><tr><td>fortitoken</td><td>Use FortiToken or FortiToken mobile two-factor authentication.</td></tr><tr><td>fortitoken-cloud</td><td>FortiToken Cloud Service.</td></tr><tr><td>email</td><td>Send a two-factor authentication code to the configured email-to email address.</td></tr><tr><td>sms</td><td>Send a two-factor authentication code to the configured sms-server and sms-phone.</td></tr></table>				Option	Description	disable	Disable two-factor authentication.	fortitoken	Use FortiToken or FortiToken mobile two-factor authentication.	fortitoken-cloud	FortiToken Cloud Service.	email	Send a two-factor authentication code to the configured email-to email address.	sms	Send a two-factor authentication code to the configured sms-server and sms-phone.
Option	Description															
disable	Disable two-factor authentication.															
fortitoken	Use FortiToken or FortiToken mobile two-factor authentication.															
fortitoken-cloud	FortiToken Cloud Service.															
email	Send a two-factor authentication code to the configured email-to email address.															
sms	Send a two-factor authentication code to the configured sms-server and sms-phone.															
two-factor-authentication	Authentication method by FortiToken Cloud.	option	-													
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>fortitoken</td><td>FortiToken authentication.</td></tr><tr><td>email</td><td>Email one time password.</td></tr><tr><td>sms</td><td>SMS one time password.</td></tr></table>				Option	Description	fortitoken	FortiToken authentication.	email	Email one time password.	sms	SMS one time password.				
Option	Description															
fortitoken	FortiToken authentication.															
email	Email one time password.															
sms	SMS one time password.															
two-factor-notification	Notification method for user activation by FortiToken Cloud.	option	-													

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>email</i>	Email notification for activation code.		
	<i>sms</i>	SMS notification for activation code.		
vdom <name>	Virtual domain(s) that the administrator can access. Virtual domain name.	string	Maximum length: 79	
wildcard	Enable/disable wildcard RADIUS authentication.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable username wildcard.		
	<i>disable</i>	Disable username wildcard.		

## config system affinity-interrupt



This command is available for model(s): FortiGate VM64.

It is not available for: FortiGate 1000D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

Configure interrupt affinity.

```
config system affinity-interrupt
  Description: Configure interrupt affinity.
  edit <id>
    set interrupt {string}
```

```

        set affinity-cpumask {string}
    next
end

```

## config system affinity-interrupt

Parameter	Description	Type	Size	Default
id	ID of the interrupt affinity setting.	integer	Minimum value: 0 Maximum value: 4294967295	0
interrupt	Interrupt name.	string	Maximum length: 127	
affinity-cpumask	Affinity setting for VM throughput (64-bit hexadecimal value in the format of 0xxxxxxxxxxxxxxxxx).	string	Maximum length: 127	

## config system affinity-packet-redistribution



This command is available for model(s): FortiGate VM64.

It is not available for: FortiGate 1000D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

Configure packet redistribution.

```

config system affinity-packet-redistribution
    Description: Configure packet redistribution.

```

```

edit <id>
    set interface {string}
    set rxqid {integer}
    set affinity-cpumask {string}
next
end

```

## config system affinity-packet-redistribution

Parameter	Description	Type	Size	Default
id	ID of the packet redistribution setting.	integer	Minimum value: 0 Maximum value: 4294967295	0
interface	Physical interface name on which to perform packet redistribution.	string	Maximum length: 127	
rxqid	ID of the receive queue (when the interface has multiple queues) on which to perform packet redistribution.	integer	Minimum value: 0 Maximum value: 255	0
affinity-cpumask	Affinity setting for VM throughput (64-bit hexadecimal value in the format of 0xxxxxxxxxxxxxxxxx).	string	Maximum length: 127	

## config system alarm

Configure alarm.

```

config system alarm
    Description: Configure alarm.
    set audible [enable|disable]
    config groups
        Description: Alarm groups.
        edit <id>
            set period {integer}
            set admin-auth-failure-threshold {integer}
            set admin-auth-lockout-threshold {integer}
            set user-auth-failure-threshold {integer}
            set user-auth-lockout-threshold {integer}
            set replay-attempt-threshold {integer}
            set self-test-failure-threshold {integer}
            set log-full-warning-threshold {integer}
            set encryption-failure-threshold {integer}
            set decryption-failure-threshold {integer}
            config fw-policy-violations
                Description: Firewall policy violations.
                edit <id>
                    set threshold {integer}
                    set src-ip {ipv4-address}

```

```

        set dst-ip {ipv4-address}
        set src-port {integer}
        set dst-port {integer}
    next
end
set fw-policy-id {integer}
set fw-policy-id-threshold {integer}
next
end
set status [enable|disable]
end

```

## config system alarm

Parameter	Description	Type	Size	Default						
audible	Enable/disable audible alarm.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable audible alarm.</td></tr><tr><td><i>disable</i></td><td>Disable audible alarm.</td></tr></table>	Option	Description	<i>enable</i>	Enable audible alarm.	<i>disable</i>	Disable audible alarm.			
Option	Description									
<i>enable</i>	Enable audible alarm.									
<i>disable</i>	Disable audible alarm.									
status	Enable/disable alarm.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable alarm.</td></tr><tr><td><i>disable</i></td><td>Disable alarm.</td></tr></table>	Option	Description	<i>enable</i>	Enable alarm.	<i>disable</i>	Disable alarm.			
Option	Description									
<i>enable</i>	Enable alarm.									
<i>disable</i>	Disable alarm.									

## config groups

Parameter	Description	Type	Size	Default
id	Group ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
period	Time period in seconds (0 = from start up).	integer	Minimum value: 0 Maximum value: 4294967295	0
admin-auth-failure-threshold	Admin authentication failure threshold.	integer	Minimum value: 0 Maximum value: 1024	0



Parameter	Description	Type	Size	Default
admin-auth-lockout-threshold	Admin authentication lockout threshold.	integer	Minimum value: 0 Maximum value: 1024	0
user-auth-failure-threshold	User authentication failure threshold.	integer	Minimum value: 0 Maximum value: 1024	0
user-auth-lockout-threshold	User authentication lockout threshold.	integer	Minimum value: 0 Maximum value: 1024	0
replay-attempt-threshold	Replay attempt threshold.	integer	Minimum value: 0 Maximum value: 1024	0
self-test-failure-threshold	Self-test failure threshold.	integer	Minimum value: 0 Maximum value: 1	0
log-full-warning-threshold	Log full warning threshold.	integer	Minimum value: 0 Maximum value: 1024	0
encryption-failure-threshold	Encryption failure threshold.	integer	Minimum value: 0 Maximum value: 1024	0
decryption-failure-threshold	Decryption failure threshold.	integer	Minimum value: 0 Maximum value: 1024	0
fw-policy-id	Firewall policy ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
fw-policy-id-threshold	Firewall policy ID threshold.	integer	Minimum value: 0 Maximum value: 1024	0

## config fw-policy-violations

Parameter	Description	Type	Size	Default
id	Firewall policy violations ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
threshold	Firewall policy violation threshold.	integer	Minimum value: 0 Maximum value: 1024	0
src-ip	Source IP (0=all).	ipv4-address	Not Specified	0.0.0.0
dst-ip	Destination IP (0=all).	ipv4-address	Not Specified	0.0.0.0
src-port	Source port (0=all).	integer	Minimum value: 0 Maximum value: 65535	0
dst-port	Destination port (0=all).	integer	Minimum value: 0 Maximum value: 65535	0

## config system alias

Configure alias command.

```
config system alias
    Description: Configure alias command.
    edit <name>
        set command {var-string}
    next
end
```

## config system alias

Parameter	Description	Type	Size	Default
command	Command list to execute.	var-string	Maximum length: 255	
name	Alias command name.	string	Maximum length: 35	

## config system api-user

Configure API users.

```
config system api-user
  Description: Configure API users.
  edit <name>
    set accprofile {string}
    set api-key {password-2}
    set comments {var-string}
    set cors-allow-origin {string}
    set peer-auth [enable|disable]
    set peer-group {string}
    set schedule {string}
    config trusthost
      Description: Trusthost.
      edit <id>
        set type [ipv4-trusthost|ipv6-trusthost]
        set ipv4-trusthost {ipv4-classnet}
        set ipv6-trusthost {ipv6-prefix}
      next
    end
  set vdom <name1>, <name2>, ...
next
end
```

## config system api-user

Parameter	Description	Type	Size	Default
accprofile	Admin user access profile.	string	Maximum length: 35	
api-key	Admin user password.	password-2	Not Specified	
comments	Comment.	var-string	Maximum length: 255	
cors-allow-origin	Value for Access-Control-Allow-Origin on API responses. Avoid using '*' if possible.	string	Maximum length: 269	
name	User name.	string	Maximum length: 35	
peer-auth	Enable/disable peer authentication.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable peer.		
	<i>disable</i>	Disable peer.		

Parameter	Description	Type	Size	Default
peer-group	Peer group name.	string	Maximum length: 35	
schedule	Schedule name.	string	Maximum length: 35	
vdom <name>	Virtual domains. Virtual domain name.	string	Maximum length: 79	

## config trusthost

Parameter	Description	Type	Size	Default						
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0						
type	Trusthost type.	option	-	ipv4-trusthost						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ipv4-trusthost</td><td>IPv4 trusthost.</td></tr><tr><td>ipv6-trusthost</td><td>IPv6 trusthost.</td></tr></table>				Option	Description	ipv4-trusthost	IPv4 trusthost.	ipv6-trusthost	IPv6 trusthost.
	Option	Description								
	ipv4-trusthost	IPv4 trusthost.								
ipv6-trusthost	IPv6 trusthost.									
ipv4-trusthost	IPv4 trusted host address.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0						
ipv6-trusthost	IPv6 trusted host address.	ipv6-prefix	Not Specified	::/0						

## config system arp-table

Configure ARP table.

```

config system arp-table
    Description: Configure ARP table.
    edit <id>
        set interface {string}
        set ip {ipv4-address}
        set mac {mac-address}
    next
end

```

## config system arp-table

Parameter	Description	Type	Size	Default
id	Unique integer ID of the entry.	integer	Minimum value: 0 Maximum value: 4294967295	0
interface	Interface name.	string	Maximum length: 15	
ip	IP address.	ipv4-address	Not Specified	0.0.0.0
mac	MAC address.	mac-address	Not Specified	00:00:00:00:00:00

## config system auto-install

Configure USB auto installation.

```
config system auto-install
    Description: Configure USB auto installation.
    set auto-install-config [enable|disable]
    set auto-install-image [enable|disable]
    set default-config-file {string}
    set default-image-file {string}
end
```

## config system auto-install

Parameter	Description	Type	Size	Default						
auto-install-config	Enable/disable auto install the config in USB disk.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable config.</td></tr><tr><td><i>disable</i></td><td>Disable config.</td></tr></table>	Option	Description	<i>enable</i>	Enable config.	<i>disable</i>	Disable config.			
Option	Description									
<i>enable</i>	Enable config.									
<i>disable</i>	Disable config.									
auto-install-image	Enable/disable auto install the image in USB disk.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable config.</td></tr><tr><td><i>disable</i></td><td>Disable config.</td></tr></table>	Option	Description	<i>enable</i>	Enable config.	<i>disable</i>	Disable config.			
Option	Description									
<i>enable</i>	Enable config.									
<i>disable</i>	Disable config.									

Parameter	Description	Type	Size	Default
default-config-file	Default config file name in USB disk.	string	Maximum length: 127	fgt_system.conf
default-image-file	Default image file name in USB disk.	string	Maximum length: 127	image.out

## config system auto-script

Configure auto script.

```
config system auto-script
    Description: Configure auto script.
    edit <name>
        set interval {integer}
        set output-size {integer}
        set repeat {integer}
        set script {var-string}
        set start [manual|auto]
        set timeout {integer}
    next
end
```

## config system auto-script

Parameter	Description	Type	Size	Default
interval	Repeat interval in seconds.	integer	Minimum value: 0 Maximum value: 31557600	0
name	Auto script name.	string	Maximum length: 35	
output-size	Number of megabytes to limit script output to.	integer	Minimum value: 10 Maximum value: 1024	10
repeat	Number of times to repeat this script (0 = infinite).	integer	Minimum value: 0 Maximum value: 65535	1
script	List of FortiOS CLI commands to repeat.	var-string	Maximum length: 1023	

Parameter	Description	Type	Size	Default
start	Script starting mode.	option	-	manual
	<b>Option</b>	<b>Description</b>		
	<i>manual</i>	Starting manually.		
	<i>auto</i>	Starting automatically.		
timeout	Maximum running time for this script in seconds (0 = no timeout).	integer	Minimum value: 0 Maximum value: 300	0

## config system automation-action

Action for automation stitches.

```
config system automation-action
  Description: Action for automation stitches.
  edit <name>
    set accprofile {string}
    set action-type [email|fortiexplorer-notification|...]
    set alicloud-access-key-id {string}
    set alicloud-access-key-secret {password}
    set alicloud-function-authorization [anonymous|function]
    set aws-api-key {password}
    set azure-api-key {password}
    set azure-function-authorization [anonymous|function|...]
    set description {var-string}
    set email-from {var-string}
    set email-subject {var-string}
    set email-to <name1>, <name2>, ...
    set execute-security-fabric [enable|disable]
    set http-body {var-string}
    config http-headers
      Description: Request headers.
      edit <id>
        set key {var-string}
        set value {var-string}
      next
    end
    set message {string}
    set message-type [text|json]
    set method [post|put|...]
    set minimum-interval {integer}
    set port {integer}
    set protocol [http|https]
    set replacement-message [enable|disable]
    set replacemsg-group {string}
    set script {var-string}
    set sdn-connector <name1>, <name2>, ...
    set security-tag {string}
```

```

        set tls-certificate {string}
        set uri {var-string}
        set verify-host-cert [enable|disable]
    next
end

```

## config system automation-action

Parameter	Description	Type	Size	Default
accprofile	Access profile for CLI script action to access FortiGate features.	string	Maximum length: 35	
action-type	Action type.	option	-	alert
	<b>Option</b>	<b>Description</b>		
	email	Send notification email.		
	fortiexplorer-notification	Send push notification to FortiExplorer.		
	alert	Generate FortiOS dashboard alert.		
	disable-ssid	Disable interface.		
	quarantine	Quarantine host.		
	quarantine-forticlient	Quarantine FortiClient by EMS.		
	quarantine-nsx	Quarantine NSX instance.		
	quarantine-fortinac	Quarantine host by FortiNAC.		
	ban-ip	Ban IP address.		
	aws-lambda	Send log data to integrated AWS service.		
	azure-function	Send log data to an Azure function.		
	google-cloud-function	Send log data to a Google Cloud function.		
	alicloud-function	Send log data to an AliCloud function.		
	webhook	Send an HTTP request.		
	cli-script	Run CLI script.		
	slack-notification	Send a notification message to a Slack incoming webhook.		
	microsoft-teams-notification	Send a notification message to a Microsoft Teams incoming webhook.		



Parameter	Description	Type	Size	Default								
alicloud-access-key-id	AliCloud AccessKey ID.	string	Maximum length: 35									
alicloud-access-key-secret	AliCloud AccessKey secret.	password	Not Specified									
alicloud-function-authorization	AliCloud function authorization type.	option	-	anonymous								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>anonymous</i></td><td>Anonymous authorization (No authorization required).</td></tr><tr><td><i>function</i></td><td>Function authorization (Authorization required).</td></tr></table>				Option	Description	<i>anonymous</i>	Anonymous authorization (No authorization required).	<i>function</i>	Function authorization (Authorization required).		
Option	Description											
<i>anonymous</i>	Anonymous authorization (No authorization required).											
<i>function</i>	Function authorization (Authorization required).											
aws-api-key	AWS API Gateway API key.	password	Not Specified									
azure-api-key	Azure function API key.	password	Not Specified									
azure-function-authorization	Azure function authorization level.	option	-	anonymous								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>anonymous</i></td><td>Anonymous authorization level (No authorization required).</td></tr><tr><td><i>function</i></td><td>Function authorization level (Function or Host Key required).</td></tr><tr><td><i>admin</i></td><td>Admin authorization level (Master Host Key required).</td></tr></table>				Option	Description	<i>anonymous</i>	Anonymous authorization level (No authorization required).	<i>function</i>	Function authorization level (Function or Host Key required).	<i>admin</i>	Admin authorization level (Master Host Key required).
Option	Description											
<i>anonymous</i>	Anonymous authorization level (No authorization required).											
<i>function</i>	Function authorization level (Function or Host Key required).											
<i>admin</i>	Admin authorization level (Master Host Key required).											
description	Description.	var-string	Maximum length: 255									
email-from	Email sender name.	var-string	Maximum length: 127									
email-subject	Email subject.	var-string	Maximum length: 511									
email-to <name>	Email addresses. Email address.	string	Maximum length: 255									
execute-security-fabric	Enable/disable execution of CLI script on all or only one FortiGate unit in the Security Fabric.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>CLI script executes on all FortiGate units in the Security Fabric.</td></tr><tr><td><i>disable</i></td><td>CLI script executes only on the FortiGate unit that the stitch is triggered.</td></tr></table>				Option	Description	<i>enable</i>	CLI script executes on all FortiGate units in the Security Fabric.	<i>disable</i>	CLI script executes only on the FortiGate unit that the stitch is triggered.		
Option	Description											
<i>enable</i>	CLI script executes on all FortiGate units in the Security Fabric.											
<i>disable</i>	CLI script executes only on the FortiGate unit that the stitch is triggered.											

Parameter	Description	Type	Size	Default
http-body	Request body (if necessary). Should be serialized json string.	var-string	Maximum length: 4095	
message	Message content.	string	Maximum length: 4095	%%log%%
message-type	Message type.	option	-	text
	Option	Description		
	text	Plaintext.		
	json	Custom JSON.		
method	Request method (POST, PUT, GET, PATCH or DELETE).	option	-	post
	Option	Description		
	post	POST.		
	put	PUT.		
	get	GET.		
	patch	PATCH.		
	delete	DELETE.		
minimum-interval	Limit execution to no more than once in this interval (in seconds).	integer	Minimum value: 0 Maximum value: 2592000	0
name	Name.	string	Maximum length: 64	
port	Protocol port.	integer	Minimum value: 1 Maximum value: 65535	0
protocol	Request protocol.	option	-	http
	Option	Description		
	http	HTTP.		
	https	HTTPS.		

Parameter	Description	Type	Size	Default						
replacement-message	Enable/disable replacement message.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable replacement message.</td></tr><tr><td><i>disable</i></td><td>Disable replacement message.</td></tr></table>	Option	Description	<i>enable</i>	Enable replacement message.	<i>disable</i>	Disable replacement message.			
Option	Description									
<i>enable</i>	Enable replacement message.									
<i>disable</i>	Disable replacement message.									
replacemsg-group	Replacement message group.	string	Maximum length: 35							
script	CLI script.	var-string	Maximum length: 1023							
sdn-connector <name>	NSX SDN connector names. SDN connector name.	string	Maximum length: 79							
security-tag	NSX security tag.	string	Maximum length: 255							
tls-certificate	Custom TLS certificate for API request.	string	Maximum length: 35							
uri	Request API URI.	var-string	Maximum length: 1023							
verify-host-cert	Enable/disable verification of the remote host certificate.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable verification of the remote host certificate.</td></tr><tr><td><i>disable</i></td><td>Disable verification of the remote host certificate.</td></tr></table>	Option	Description	<i>enable</i>	Enable verification of the remote host certificate.	<i>disable</i>	Disable verification of the remote host certificate.			
Option	Description									
<i>enable</i>	Enable verification of the remote host certificate.									
<i>disable</i>	Disable verification of the remote host certificate.									

## config http-headers

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
key	Request header key.	var-string	Maximum length: 1023	
value	Request header value.	var-string	Maximum length: 4095	

## config system automation-destination

Automation destinations.

```
config system automation-destination
  Description: Automation destinations.
  edit <name>
    set destination <name1>, <name2>, ...
    set ha-group-id {integer}
    set type [fortigate|ha-cluster]
  next
end
```

## config system automation-destination

Parameter	Description	Type	Size	Default
destination <name>	Destinations. Destination.	string	Maximum length: 31	
ha-group-id	Cluster group ID set for this destination.	integer	Minimum value: 0 Maximum value: 255	0
name	Name.	string	Maximum length: 35	
type	Destination type.	option	-	fortigate
		Option	Description	
		<i>fortigate</i>	FortiGate set as destination.	
		<i>ha-cluster</i>	HA cluster set as destination.	

## config system automation-stitch

Automation stitches.

```
config system automation-stitch
  Description: Automation stitches.
  edit <name>
    config actions
      Description: Configure stitch actions.
      edit <id>
        set action {string}
        set delay {integer}
        set required [enable|disable]
      next
    end
    set description {var-string}
    set destination <name1>, <name2>, ...
```

```

        set status [enable|disable]
        set trigger {string}
    next
end

```

## config system automation-stitch

Parameter	Description	Type	Size	Default
description	Description.	var-string	Maximum length: 255	
destination <name>	Serial number/HA group-name of destination devices. Destination name.	string	Maximum length: 79	
name	Name.	string	Maximum length: 35	
status	Enable/disable this stitch.	option	-	enable
	Option	Description		
	enable	Enable stitch.		
	disable	Disable stitch.		
trigger	Trigger name.	string	Maximum length: 35	

## config actions

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
action	Action name.	string	Maximum length: 64	
delay	Delay before execution (in seconds).	integer	Minimum value: 0 Maximum value: 3600	0
required	Required in action chain.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Required in action chain.		
	<i>disable</i>	Not required in action chain.		

## config system automation-trigger

Trigger for automation stitches.

```
config system automation-trigger
  Description: Trigger for automation stitches.
  edit <name>
    set description {var-string}
    set event-type [ioc|event-log|...]
    set fabric-event-name {var-string}
    set fabric-event-severity {var-string}
    set faz-event-name {var-string}
    set faz-event-severity {var-string}
    set faz-event-tags {var-string}
    config fields
      Description: Customized trigger field settings.
      edit <id>
        set name {string}
        set value {var-string}
      next
    end
    set license-type [forticare-support|fortiguard-webfilter|...]
    set logid <id1>, <id2>, ...
    set report-type [posture|coverage|...]
    set serial {var-string}
    set trigger-day {integer}
    set trigger-frequency [hourly|daily|...]
    set trigger-hour {integer}
    set trigger-minute {integer}
    set trigger-type [event-based|scheduled]
    set trigger-weekday [sunday|monday|...]
  next
end
```

## config system automation-trigger

Parameter	Description	Type	Size	Default
description	Description.	var-string	Maximum length: 255	
event-type	Event type.	option	-	ioc
	Option	Description		
	ioc	Indicator of compromise detected.		
	event-log	Use log ID as trigger.		
	reboot	Device reboot.		
	low-memory	Conserve mode due to low memory.		
	high-cpu	High CPU usage.		

Parameter	Description	Type	Size	Default																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>license-near-expiry</i></td><td>License near expiration date.</td></tr><tr><td><i>ha-failover</i></td><td>HA failover.</td></tr><tr><td><i>config-change</i></td><td>Configuration change.</td></tr><tr><td><i>security-rating-summary</i></td><td>Security rating summary.</td></tr><tr><td><i>virus-ips-db-updated</i></td><td>Virus and IPS database updated.</td></tr><tr><td><i>faz-event</i></td><td>FortiAnalyzer event.</td></tr><tr><td><i>incoming-webhook</i></td><td>Incoming webhook call.</td></tr><tr><td><i>fabric-event</i></td><td>Fabric connector event.</td></tr></table>	Option	Description	<i>license-near-expiry</i>	License near expiration date.	<i>ha-failover</i>	HA failover.	<i>config-change</i>	Configuration change.	<i>security-rating-summary</i>	Security rating summary.	<i>virus-ips-db-updated</i>	Virus and IPS database updated.	<i>faz-event</i>	FortiAnalyzer event.	<i>incoming-webhook</i>	Incoming webhook call.	<i>fabric-event</i>	Fabric connector event.			
	Option	Description																				
	<i>license-near-expiry</i>	License near expiration date.																				
	<i>ha-failover</i>	HA failover.																				
	<i>config-change</i>	Configuration change.																				
	<i>security-rating-summary</i>	Security rating summary.																				
	<i>virus-ips-db-updated</i>	Virus and IPS database updated.																				
	<i>faz-event</i>	FortiAnalyzer event.																				
	<i>incoming-webhook</i>	Incoming webhook call.																				
<i>fabric-event</i>	Fabric connector event.																					
fabric-event-name	Fabric connector event handler name.	var-string	Maximum length: 255																			
fabric-event-severity	Fabric connector event severity.	var-string	Maximum length: 255																			
faz-event-name	FortiAnalyzer event handler name.	var-string	Maximum length: 255																			
faz-event-severity	FortiAnalyzer event severity.	var-string	Maximum length: 255																			
faz-event-tags	FortiAnalyzer event tags.	var-string	Maximum length: 255																			
license-type	License type.	option	-	forticare-support																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>forticare-support</i></td><td>FortiCare support license.</td></tr><tr><td><i>fortiguard-webfilter</i></td><td>FortiGuard web filter license.</td></tr><tr><td><i>fortiguard-antispam</i></td><td>FortiGuard antispam license.</td></tr><tr><td><i>fortiguard-antivirus</i></td><td>FortiGuard AntiVirus license.</td></tr><tr><td><i>fortiguard-ips</i></td><td>FortiGuard IPS license.</td></tr></table>	Option	Description	<i>forticare-support</i>	FortiCare support license.	<i>fortiguard-webfilter</i>	FortiGuard web filter license.	<i>fortiguard-antispam</i>	FortiGuard antispam license.	<i>fortiguard-antivirus</i>	FortiGuard AntiVirus license.	<i>fortiguard-ips</i>	FortiGuard IPS license.									
	Option	Description																				
	<i>forticare-support</i>	FortiCare support license.																				
	<i>fortiguard-webfilter</i>	FortiGuard web filter license.																				
	<i>fortiguard-antispam</i>	FortiGuard antispam license.																				
	<i>fortiguard-antivirus</i>	FortiGuard AntiVirus license.																				
<i>fortiguard-ips</i>	FortiGuard IPS license.																					

Parameter	Description	Type	Size	Default										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>fortiguard-management</i></td><td>FortiGuard management service license.</td></tr><tr><td><i>forticloud</i></td><td>FortiCloud license.</td></tr><tr><td><i>any</i></td><td>Any license.</td></tr></table>	Option	Description	<i>fortiguard-management</i>	FortiGuard management service license.	<i>forticloud</i>	FortiCloud license.	<i>any</i>	Any license.					
	Option	Description												
	<i>fortiguard-management</i>	FortiGuard management service license.												
	<i>forticloud</i>	FortiCloud license.												
<i>any</i>	Any license.													
logid <id>	Log IDs to trigger event. Log ID.	integer	Minimum value: 1 Maximum value: 65535											
name	Name.	string	Maximum length: 35											
report-type	Security Rating report.	option	-	posture										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>posture</i></td><td>Posture report.</td></tr><tr><td><i>coverage</i></td><td>Coverage report.</td></tr><tr><td><i>optimization</i></td><td>Optimization report</td></tr><tr><td><i>any</i></td><td>Any report.</td></tr></table>	Option	Description	<i>posture</i>	Posture report.	<i>coverage</i>	Coverage report.	<i>optimization</i>	Optimization report	<i>any</i>	Any report.			
	Option	Description												
	<i>posture</i>	Posture report.												
	<i>coverage</i>	Coverage report.												
	<i>optimization</i>	Optimization report												
<i>any</i>	Any report.													
serial	Fabric connector serial number.	var-string	Maximum length: 255											
trigger-day	Day within a month to trigger.	integer	Minimum value: 1 Maximum value: 31	1										
trigger-frequency	Scheduled trigger frequency.	option	-	daily										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>hourly</i></td><td>Run hourly.</td></tr><tr><td><i>daily</i></td><td>Run daily.</td></tr><tr><td><i>weekly</i></td><td>Run weekly.</td></tr><tr><td><i>monthly</i></td><td>Run monthly.</td></tr></table>	Option	Description	<i>hourly</i>	Run hourly.	<i>daily</i>	Run daily.	<i>weekly</i>	Run weekly.	<i>monthly</i>	Run monthly.			
	Option	Description												
	<i>hourly</i>	Run hourly.												
	<i>daily</i>	Run daily.												
	<i>weekly</i>	Run weekly.												
<i>monthly</i>	Run monthly.													



Parameter	Description	Type	Size	Default
trigger-hour	Hour of the day on which to trigger.	integer	Minimum value: 0 Maximum value: 23	0
trigger-minute	Minute of the hour on which to trigger.	integer	Minimum value: 0 Maximum value: 59	0
trigger-type	Trigger type.	option	-	event-based
	<b>Option</b>		<b>Description</b>	
	<i>event-based</i>		Event based trigger.	
	<i>scheduled</i>		Scheduled trigger.	
trigger-weekday	Day of week for trigger.	option	-	
	<b>Option</b>		<b>Description</b>	
	<i>sunday</i>		Sunday.	
	<i>monday</i>		Monday.	
	<i>tuesday</i>		Tuesday.	
	<i>wednesday</i>		Wednesday.	
	<i>thursday</i>		Thursday.	
	<i>friday</i>		Friday.	
	<i>saturday</i>		Saturday.	

## config fields

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
name	Name.	string	Maximum length: 35	
value	Value.	var-string	Maximum length: 63	

## config system autoupdate schedule

Configure update schedule.

```
config system autoupdate schedule
  Description: Configure update schedule.
  set day [Sunday|Monday|...]
  set frequency [every|daily|...]
  set status [enable|disable]
  set time {user}
end
```

## config system autoupdate schedule

Parameter	Description	Type	Size	Default
day	Update day.	option	-	Monday
	<b>Option</b>	<b>Description</b>		
	<i>Sunday</i>	Update every Sunday.		
	<i>Monday</i>	Update every Monday.		
	<i>Tuesday</i>	Update every Tuesday.		
	<i>Wednesday</i>	Update every Wednesday.		
	<i>Thursday</i>	Update every Thursday.		
	<i>Friday</i>	Update every Friday.		
	<i>Saturday</i>	Update every Saturday.		
frequency	Update frequency.	option	-	automatic
	<b>Option</b>	<b>Description</b>		
	<i>every</i>	Time interval.		
	<i>daily</i>	Every day.		
	<i>weekly</i>	Every week.		
	<i>automatic</i>	Update automatically within every one hour period.		
status	Enable/disable scheduled updates.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
time	Update time.	user	Not Specified	

## config system autoupdate tunneling

Configure web proxy tunneling for the FDN.

```
config system autoupdate tunneling
    Description: Configure web proxy tunneling for the FDN.
    set address {string}
    set password {password}
    set port {integer}
    set status [enable|disable]
    set username {string}
end
```

## config system autoupdate tunneling

Parameter	Description	Type	Size	Default
address	Web proxy IP address or FQDN.	string	Maximum length: 63	
password	Web proxy password.	password	Not Specified	
port	Web proxy port.	integer	Minimum value: 0 Maximum value: 65535	0
status	Enable/disable web proxy tunneling.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
username	Web proxy username.	string	Maximum length: 49	

## config system bypass



This command is available for model(s): FortiGate 2500E, FortiGate 400E Bypass, FortiGate 800D, FortiGate 80F Bypass, FortiGateRugged 60F 3G4G, FortiGateRugged 60F.

It is not available for: FortiGate 1000D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3960E, FortiGate 3980E, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate VM64, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

Configure system bypass.

```
config system bypass
    Description: Configure system bypass.
    set auto-recover [enable|disable]
    set bypass-timeout [2|4|...]
    set bypass-watchdog [enable|disable]
    set poweroff-bypass [enable|disable]
end
```

## config system bypass

Parameter	Description	Type	Size	Default						
auto-recover *	Automatically recover from bypass mode after system reboot.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Recover interfaces from bypass mode. The actual mode is determined by poweron-bypass setting.</td></tr><tr><td><i>disable</i></td><td>Keep interfaces in bypass mode if bypass was previously triggered.</td></tr></table>	Option	Description	<i>enable</i>	Recover interfaces from bypass mode. The actual mode is determined by poweron-bypass setting.	<i>disable</i>	Keep interfaces in bypass mode if bypass was previously triggered.			
Option	Description									
<i>enable</i>	Recover interfaces from bypass mode. The actual mode is determined by poweron-bypass setting.									
<i>disable</i>	Keep interfaces in bypass mode if bypass was previously triggered.									

Parameter	Description	Type	Size	Default																
bypass-timeout *	timeout setting for bypass watchdog	option	-	10																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>2</td><td>2 second</td></tr><tr><td>4</td><td>4 second</td></tr><tr><td>6</td><td>6 second</td></tr><tr><td>8</td><td>8 second</td></tr><tr><td>10</td><td>10 second</td></tr><tr><td>12</td><td>12 second</td></tr><tr><td>14</td><td>14 second</td></tr></table>	Option	Description	2	2 second	4	4 second	6	6 second	8	8 second	10	10 second	12	12 second	14	14 second			
Option	Description																			
2	2 second																			
4	4 second																			
6	6 second																			
8	8 second																			
10	10 second																			
12	12 second																			
14	14 second																			
bypass-watchdog	watchdog to bypass interfaces in case of software/hardware failure	option	-	disable																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable watchdog for bypass interfaces.</td></tr><tr><td><i>disable</i></td><td>Disable watchdog for bypass interfaces.</td></tr></table>	Option	Description	<i>enable</i>	Enable watchdog for bypass interfaces.	<i>disable</i>	Disable watchdog for bypass interfaces.													
Option	Description																			
<i>enable</i>	Enable watchdog for bypass interfaces.																			
<i>disable</i>	Disable watchdog for bypass interfaces.																			
poweroff-bypass *	set interface bypass state in power off	option	-	disable																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable bypass when power off.</td></tr><tr><td><i>disable</i></td><td>Disable bypass when power off.</td></tr></table>	Option	Description	<i>enable</i>	Enable bypass when power off.	<i>disable</i>	Disable bypass when power off.													
Option	Description																			
<i>enable</i>	Enable bypass when power off.																			
<i>disable</i>	Disable bypass when power off.																			

\* This parameter may not exist in some models.

## config system central-management

Configure central management.

```
config system central-management
  Description: Configure central management.
  set allow-monitor [enable|disable]
  set allow-push-configuration [enable|disable]
  set allow-push-firmware [enable|disable]
  set allow-remote-firmware-upgrade [enable|disable]
  set allow-remote-lte-firmware-upgrade [enable|disable]
  set ca-cert {user}
  set enc-algorithm [default|high|...]
  set fmg {user}
  set fmg-source-ip {ipv4-address}
```

```

set fmg-source-ip6 {ipv6-address}
set fmg-update-port [8890|443]
set include-default-servers [enable|disable]
set interface {string}
set interface-select-method [auto|sdwan|...]
set local-cert {string}
set ltefw-upgrade-frequency [everyHour|every12hour|...]
set ltefw-upgrade-time {string}
set mode [normal|backup]
set schedule-config-restore [enable|disable]
set schedule-script-restore [enable|disable]
set serial-number {user}
config server-list
    Description: Additional servers that the FortiGate can use for updates (for AV, IPS,
updates) and ratings (for web filter and antispam ratings) servers.
    edit <id>
        set server-type {option1}, {option2}, ...
        set addr-type [ipv4|ipv6|...]
        set server-address {ipv4-address}
        set server-address6 {ipv6-address}
        set fqdn {string}
    next
end
set type [fortimanager|fortiguard|...]
set use-elbc-vdom [enable|disable]
set vdom {string}
end

```

## config system central-management

Parameter	Description	Type	Size	Default
allow-monitor	Enable/disable allowing the central management server to remotely monitor this FortiGate unit.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable remote monitoring of device.		
	<i>disable</i>	Disable remote monitoring of device.		
allow-push-configuration	Enable/disable allowing the central management server to push configuration changes to this FortiGate.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable push configuration.		
	<i>disable</i>	Disable push configuration.		
allow-push-firmware	Enable/disable allowing the central management server to push firmware updates to this FortiGate.	option	-	enable

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable push firmware.		
	<i>disable</i>	Disable push firmware.		
allow-remote-firmware-upgrade	Enable/disable remotely upgrading the firmware on this FortiGate from the central management server.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable remote firmware upgrade.		
	<i>disable</i>	Disable remote firmware upgrade.		
allow-remote-lte-firmware-upgrade *	Enable/disable remotely upgrading the lte firmware on this FortiGate from the central management server.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable remote lte firmware upgrade.		
	<i>disable</i>	Disable remote lte firmware upgrade.		
ca-cert	CA certificate to be used by FGFM protocol.	user	Not Specified	
enc-algorithm	Encryption strength for communications between the FortiGate and central management.	option	-	high
	<b>Option</b>	<b>Description</b>		
	<i>default</i>	High strength algorithms and medium-strength 128-bit key length algorithms.		
	<i>high</i>	128-bit and larger key length algorithms.		
	<i>low</i>	64-bit or 56-bit key length algorithms without export restrictions.		
fmg	IP address or FQDN of the FortiManager.	user	Not Specified	
fmg-source-ip	IPv4 source address that this FortiGate uses when communicating with FortiManager.	ipv4-address	Not Specified	0.0.0.0
fmg-source-ip6	IPv6 source address that this FortiGate uses when communicating with FortiManager.	ipv6-address	Not Specified	::
fmg-update-port	Port used to communicate with FortiManager that is acting as a FortiGuard update server.	option	-	8890

Parameter	Description	Type	Size	Default										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>8890</td><td>Use port 8890 to communicate with FortiManager that is acting as a FortiGuard update server.</td></tr><tr><td>443</td><td>Use port 443 to communicate with FortiManager that is acting as a FortiGuard update server.</td></tr></table>	Option	Description	8890	Use port 8890 to communicate with FortiManager that is acting as a FortiGuard update server.	443	Use port 443 to communicate with FortiManager that is acting as a FortiGuard update server.							
	Option	Description												
	8890	Use port 8890 to communicate with FortiManager that is acting as a FortiGuard update server.												
443	Use port 443 to communicate with FortiManager that is acting as a FortiGuard update server.													
include-default-servers	Enable/disable inclusion of public FortiGuard servers in the override server list.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable inclusion of public FortiGuard servers in the override server list.</td></tr><tr><td>disable</td><td>Disable inclusion of public FortiGuard servers in the override server list.</td></tr></table>	Option	Description	enable	Enable inclusion of public FortiGuard servers in the override server list.	disable	Disable inclusion of public FortiGuard servers in the override server list.							
	Option	Description												
	enable	Enable inclusion of public FortiGuard servers in the override server list.												
disable	Disable inclusion of public FortiGuard servers in the override server list.													
interface	Specify outgoing interface to reach server.	string	Maximum length: 15											
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>auto</td><td>Set outgoing interface automatically.</td></tr><tr><td>sdwan</td><td>Set outgoing interface by SD-WAN or policy routing rules.</td></tr><tr><td>specify</td><td>Set outgoing interface manually.</td></tr></table>	Option	Description	auto	Set outgoing interface automatically.	sdwan	Set outgoing interface by SD-WAN or policy routing rules.	specify	Set outgoing interface manually.					
	Option	Description												
	auto	Set outgoing interface automatically.												
	sdwan	Set outgoing interface by SD-WAN or policy routing rules.												
specify	Set outgoing interface manually.													
local-cert	Certificate to be used by FGFM protocol.	string	Maximum length: 35											
ltefw-upgrade-frequency *	Set LTE firmware auto pushdown frequency.	option	-											
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>everyHour</td><td>Auto check and pushdown LTE firmware every hour</td></tr><tr><td>every12hour</td><td>Auto check and pushdown LTE firmware every 12 hours</td></tr><tr><td>everyDay</td><td>Auto check and pushdown LTE firmware every day</td></tr><tr><td>everyWeek</td><td>Auto check and pushdown LTE firmware every week</td></tr></table>	Option	Description	everyHour	Auto check and pushdown LTE firmware every hour	every12hour	Auto check and pushdown LTE firmware every 12 hours	everyDay	Auto check and pushdown LTE firmware every day	everyWeek	Auto check and pushdown LTE firmware every week			
	Option	Description												
	everyHour	Auto check and pushdown LTE firmware every hour												
	every12hour	Auto check and pushdown LTE firmware every 12 hours												
	everyDay	Auto check and pushdown LTE firmware every day												
everyWeek	Auto check and pushdown LTE firmware every week													
ltefw-upgrade-time *	Schedule next LTE firmware upgrade time (Local Time). Format: YYYY-MM-DD HH:MM:SS	string	Maximum length: 35											
mode	Central management mode.	option	-	normal										



Parameter	Description	Type	Size	Default
	<b>Option</b> <b>Description</b>			
	<i>normal</i>	Manage and configure this FortiGate from FortiManager.		
	<i>backup</i>	Manage and configure this FortiGate locally and back up its configuration to FortiManager.		
schedule-config-restore	Enable/disable allowing the central management server to restore the configuration of this FortiGate.	option	-	enable
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Enable scheduled configuration restore.		
	<i>disable</i>	Disable scheduled configuration restore.		
schedule-script-restore	Enable/disable allowing the central management server to restore the scripts stored on this FortiGate.	option	-	enable
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Enable scheduled script restore.		
	<i>disable</i>	Disable scheduled script restore.		
serial-number	Serial number.	user	Not Specified	
type	Central management type.	option	-	none
	<b>Option</b> <b>Description</b>			
	<i>fortimanager</i>	FortiManager.		
	<i>fortiguard</i>	Central management of this FortiGate using FortiCloud.		
	<i>none</i>	No central management.		
use-elbc-vdom *	Enable/disable use of special ELBC config sync VDOM to connect to FortiManager.	option	-	disable
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	enable		
	<i>disable</i>	disable		
vdom	Virtual domain (VDOM) name to use when communicating with FortiManager.	string	Maximum length: 31	root

\* This parameter may not exist in some models.

## config server-list

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
server-type	FortiGuard service type.	option	-	
	<b>Option</b>	<b>Description</b>		
	<i>update</i>	AV, IPS, and AV-query update server.		
	<i>rating</i>	Web filter and anti-spam rating server.		
addr-type	Indicate whether the FortiGate communicates with the override server using an IPv4 address, an IPv6 address or a FQDN.	option	-	ipv4
	<b>Option</b>	<b>Description</b>		
	<i>ipv4</i>	IPv4 address.		
	<i>ipv6</i>	IPv6 address.		
	<i>fqdn</i>	FQDN.		
server-address	IPv4 address of override server.	ipv4-address	Not Specified	0.0.0.0
server-address6	IPv6 address of override server.	ipv6-address	Not Specified	::
fqdn	FQDN address of override server.	string	Maximum length: 255	

## config system cluster-sync

Configure FortiGate Session Life Support Protocol (FGSP) session synchronization.

```
config system cluster-sync
```

Description: Configure FortiGate Session Life Support Protocol (FGSP) session synchronization.

```
edit <sync-id>
    set down-intfs-before-sess-sync <name1>, <name2>, ...
    set hb-interval {integer}
    set hb-lost-threshold {integer}
    set ipsec-tunnel-sync [enable|disable]
    set peerip {ipv4-address}
    set peervd {string}
    set secondary-add-ipsec-routes [enable|disable]
config session-sync-filter
```

```

        Description: Add one or more filters if you only want to synchronize some
sessions. Use the filter to configure the types of sessions to synchronize.
        set srcintf {string}
        set dstintf {string}
        set srcaddr {ipv4-classnet-any}
        set dstaddr {ipv4-classnet-any}
        set srcaddr6 {ipv6-network}
        set dstaddr6 {ipv6-network}
        config custom-service
            Description: Only sessions using these custom services are synchronized. Use
source and destination port ranges to define these custom services.
            edit <id>
                set src-port-range {user}
                set dst-port-range {user}
            next
        end
    end
    set syncvd <name1>, <name2>, ...
next
end

```

## config system cluster-sync

Parameter	Description	Type	Size	Default						
down-intfs-before-sess-sync <name>	List of interfaces to be turned down before session synchronization is complete. Interface name.	string	Maximum length: 79							
hb-interval	Heartbeat interval. Increase to reduce false positives.	integer	Minimum value: 1 Maximum value: 20	2						
hb-lost-threshold	Lost heartbeat threshold. Increase to reduce false positives.	integer	Minimum value: 1 Maximum value: 60	10						
ipsec-tunnel-sync	Enable/disable IPsec tunnel synchronization.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable IPsec tunnel synchronization.</td></tr><tr><td><i>disable</i></td><td>Disable IPsec tunnel synchronization.</td></tr></table>				Option	Description	<i>enable</i>	Enable IPsec tunnel synchronization.	<i>disable</i>	Disable IPsec tunnel synchronization.
Option	Description									
<i>enable</i>	Enable IPsec tunnel synchronization.									
<i>disable</i>	Disable IPsec tunnel synchronization.									
peerip	IP address of the interface on the peer unit that is used for the session synchronization link.	ipv4-address	Not Specified	0.0.0.0						

Parameter	Description	Type	Size	Default
peervd	VDOM that contains the session synchronization link interface on the peer unit. Usually both peers would have the same peervd.	string	Maximum length: 31	root
secondary-add-ipsec-routes	Enable/disable IKE route announcement on the backup unit.	option	-	enable
	Option	Description		
	enable	Add IKE routes to the backup unit.		
	disable	Do not add IKE routes to the backup unit.		
sync-id	Sync ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
syncvd <name>	Sessions from these VDOMs are synchronized using this session synchronization configuration. VDOM name.	string	Maximum length: 79	

### config session-sync-filter

Parameter	Description	Type	Size	Default
srcintf	Only sessions from this interface are synchronized. You can only enter one interface name. To synchronize sessions for multiple source interfaces, add multiple filters.	string	Maximum length: 15	
dstintf	Only sessions to this interface are synchronized. You can only enter one interface name. To synchronize sessions to multiple destination interfaces, add multiple filters.	string	Maximum length: 15	
srcaddr	Only sessions from this IPv4 address are synchronized. You can only enter one address. To synchronize sessions from multiple source addresses, add multiple filters.	ipv4-classnet-any	Not Specified	0.0.0.0 0.0.0.0
dstaddr	Only sessions to this IPv4 address are synchronized. You can only enter one address. To synchronize sessions for multiple destination addresses, add multiple filters.	ipv4-classnet-any	Not Specified	0.0.0.0 0.0.0.0

Parameter	Description	Type	Size	Default
srcaddr6	Only sessions from this IPv6 address are synchronized. You can only enter one address. To synchronize sessions from multiple source addresses, add multiple filters.	ipv6-network	Not Specified	::/0
dstaddr6	Only sessions to this IPv6 address are synchronized. You can only enter one address. To synchronize sessions for multiple destination addresses, add multiple filters.	ipv6-network	Not Specified	::/0

### config custom-service

Parameter	Description	Type	Size	Default
id	Custom service ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
src-port-range	Custom service source port range.	user	Not Specified	0-0
dst-port-range	Custom service destination port range.	user	Not Specified	0-0

## config system console

Configure console.

```
config system console
    Description: Configure console.
    set baudrate [9600|19200|...]
    set fortiexplorer [enable|disable]
    set login [enable|disable]
    set mode [batch|line]
    set output [standard|more]
end
```

### config system console

Parameter	Description	Type	Size	Default						
baudrate	Console baud rate.	option	-	9600						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>9600</td><td>9600</td></tr><tr><td>19200</td><td>19200</td></tr></table>				Option	Description	9600	9600	19200	19200
	Option	Description								
	9600	9600								
19200	19200									

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>38400</i>	38400		
	<i>57600</i>	57600		
	<i>115200</i>	115200		
fortiexplorer *	Enable/disable access for FortiExplorer.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable FortiExplorer access.		
	<i>disable</i>	Disable FortiExplorer access.		
login	Enable/disable serial console and FortiExplorer.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Console login enable.		
	<i>disable</i>	Console login disable.		
mode	Console mode.	option	-	line
	<b>Option</b>	<b>Description</b>		
	<i>batch</i>	Batch mode.		
	<i>line</i>	Line mode.		
output	Console output mode.	option	-	more
	<b>Option</b>	<b>Description</b>		
	<i>standard</i>	Standard output.		
	<i>more</i>	More page output.		

\* This parameter may not exist in some models.

## config system csf

Add this FortiGate to a Security Fabric or set up a new Security Fabric on this FortiGate.

```
config system csf
    Description: Add this FortiGate to a Security Fabric or set up a new Security Fabric on
    this FortiGate.
    set accept-auth-by-cert [disable|enable]
    set authorization-request-type [serial|certificate]
    set certificate {string}
    set configuration-sync [default|local]
    set downstream-access [enable|disable]
```

```

set downstream-accprofile {string}
config fabric-connector
    Description: Fabric connector configuration.
    edit <serial>
        set accprofile {string}
        set configuration-write-access [enable|disable]
    next
end
config fabric-device
    Description: Fabric device configuration.
    edit <name>
        set device-ip {ipv4-address}
        set https-port {integer}
        set access-token {varlen_password}
    next
end
set fabric-object-unification [default|local]
set fabric-workers {integer}
set forticloud-account-enforcement [enable|disable]
set group-name {string}
set group-password {password}
set log-unification [disable|enable]
set saml-configuration-sync [default|local]
set status [enable|disable]
config trusted-list
    Description: Pre-authorized and blocked security fabric nodes.
    edit <name>
        set authorization-type [serial|certificate]
        set serial {string}
        set certificate {var-string}
        set action [accept|deny]
        set ha-members {string}
        set downstream-authorization [enable|disable]
    next
end
set upstream {string}
set upstream-port {integer}
end

```

## config system csf

Parameter	Description	Type	Size	Default
accept-auth-by-cert	Accept connections with unknown certificates and ask admin for approval.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Do not accept SSL connections with unknown certificates.		
	<i>enable</i>	Accept SSL connections without automatic certificate verification.		
authorization-request-type	Authorization request type.	option	-	serial

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>serial</i></td><td>Request verification by serial number.</td></tr><tr><td><i>certificate</i></td><td>Request verification by certificate.</td></tr></table>	Option	Description	<i>serial</i>	Request verification by serial number.	<i>certificate</i>	Request verification by certificate.			
	Option	Description								
	<i>serial</i>	Request verification by serial number.								
<i>certificate</i>	Request verification by certificate.									
certificate	Certificate.	string	Maximum length: 35							
configuration-sync	Configuration sync mode.	option	-	default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>Synchronize configuration for IPAM, FortiAnalyzer, FortiSandbox, and Central Management to root node.</td></tr><tr><td><i>local</i></td><td>Do not synchronize configuration with root node.</td></tr></table>	Option	Description	<i>default</i>	Synchronize configuration for IPAM, FortiAnalyzer, FortiSandbox, and Central Management to root node.	<i>local</i>	Do not synchronize configuration with root node.			
	Option	Description								
	<i>default</i>	Synchronize configuration for IPAM, FortiAnalyzer, FortiSandbox, and Central Management to root node.								
<i>local</i>	Do not synchronize configuration with root node.									
downstream-access	Enable/disable downstream device access to this device's configuration and data.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable downstream device access to this device's configuration and data.</td></tr><tr><td><i>disable</i></td><td>Disable downstream device access to this device's configuration and data.</td></tr></table>	Option	Description	<i>enable</i>	Enable downstream device access to this device's configuration and data.	<i>disable</i>	Disable downstream device access to this device's configuration and data.			
	Option	Description								
	<i>enable</i>	Enable downstream device access to this device's configuration and data.								
<i>disable</i>	Disable downstream device access to this device's configuration and data.									
downstream-acccprofile	Default access profile for requests from downstream devices.	string	Maximum length: 35							
fabric-object-unification	Fabric CMDB Object Unification.	option	-	default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>Global CMDB objects will be synchronized in Security Fabric.</td></tr><tr><td><i>local</i></td><td>Global CMDB objects will not be synchronized to and from this device.</td></tr></table>	Option	Description	<i>default</i>	Global CMDB objects will be synchronized in Security Fabric.	<i>local</i>	Global CMDB objects will not be synchronized to and from this device.			
	Option	Description								
	<i>default</i>	Global CMDB objects will be synchronized in Security Fabric.								
<i>local</i>	Global CMDB objects will not be synchronized to and from this device.									
fabric-workers	Number of worker processes for Security Fabric daemon.	integer	Minimum value: 1 Maximum value: 4	2						
forticloud-account-enforcement	Fabric FortiCloud account unification.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable FortiCloud account ID matching for Security Fabric.</td></tr></table>	Option	Description	<i>enable</i>	Enable FortiCloud account ID matching for Security Fabric.					
	Option	Description								
<i>enable</i>	Enable FortiCloud account ID matching for Security Fabric.									



Parameter	Description	Type	Size	Default
	<b>Option</b> <b>Description</b>			
	<i>disable</i>	Disable FortiCloud account ID matching for Security Fabric.		
group-name	Security Fabric group name. All FortiGates in a Security Fabric must have the same group name.	string	Maximum length: 35	
group-password	Security Fabric group password. All FortiGates in a Security Fabric must have the same group password.	password	Not Specified	
log-unification	Enable/disable broadcast of discovery messages for log unification.	option	-	enable
	<b>Option</b> <b>Description</b>			
	<i>disable</i>	Disable broadcast of discovery messages for log unification.		
	<i>enable</i>	Enable broadcast of discovery messages for log unification.		
saml-configuration-sync	SAML setting configuration synchronization.	option	-	default
	<b>Option</b> <b>Description</b>			
	<i>default</i>	SAML setting for fabric members is created by fabric root.		
	<i>local</i>	Do not apply SAML configuration generated by root.		
status	Enable/disable Security Fabric.	option	-	disable
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Enable Security Fabric.		
	<i>disable</i>	Disable Security Fabric.		
upstream	IP/FQDN of the FortiGate upstream from this FortiGate in the Security Fabric.	string	Maximum length: 255	
upstream-port	The port number to use to communicate with the FortiGate upstream from this FortiGate in the Security Fabric.	integer	Minimum value: 1 Maximum value: 65535	8013

### config fabric-connector

Parameter	Description	Type	Size	Default
serial	Serial.	string	Maximum length: 19	

Parameter	Description	Type	Size	Default
accprofile	Override access profile.	string	Maximum length: 35	
configuration-write-access	Enable/disable downstream device write access to configuration.	option	-	disable
	Option	Description		
	enable	Enable downstream device write access to configuration.		
	disable	Disable downstream device write access to configuration.		

### config fabric-device

Parameter	Description	Type	Size	Default
name	Device name.	string	Maximum length: 35	
device-ip	Device IP.	ipv4-address	Not Specified	0.0.0.0
https-port	HTTPS port for fabric device.	integer	Minimum value: 1 Maximum value: 65535	443
access-token	Device access token.	varlen_password	Not Specified	

### config trusted-list

Parameter	Description	Type	Size	Default
name	Name.	string	Maximum length: 35	
authorization-type	Authorization type.	option	-	serial
	<div><div>Option</div><div>Description</div></div>			
	<div><div>serial</div><div>Verify downstream by serial number.</div></div>			
	<div><div>certificate</div><div>Verify downstream by certificate.</div></div>			
serial	Serial.	string	Maximum length: 19	

Parameter	Description	Type	Size	Default
certificate	Certificate.	var-string	Maximum length: 32767	
action	Security fabric authorization action.	option	-	accept
	Option	Description		
	accept	Accept authorization request.		
	deny	Deny authorization request.		
ha-members	HA members.	string	Maximum length: 19	
downstream-authorization	Trust authorizations by this node's administrator.	option	-	disable
	Option	Description		
	enable	Enable downstream authorization.		
	disable	Disable downstream authorization.		

## config system custom-language

Configure custom languages.

```
config system custom-language
    Description: Configure custom languages.
    edit <name>
        set comments {var-string}
        set filename {string}
    next
end
```

## config system custom-language

Parameter	Description	Type	Size	Default
comments	Comment.	var-string	Maximum length: 255	
filename	Custom language file path.	string	Maximum length: 63	
name	Name.	string	Maximum length: 35	

## config system ddns

Configure DDNS.

```
config system ddns
  Description: Configure DDNS.
  edit <ddnsid>
    set addr-type [ipv4|ipv6]
    set bound-ip {string}
    set clear-text [disable|enable]
    set ddns-auth [disable|tsig]
    set ddns-domain {string}
    set ddns-key {password_aes256}
    set ddns-keyname {string}
    set ddns-password {password}
    set ddns-server [dyndns.org|dyns.net|...]
    set ddns-server-addr <addr1>, <addr2>, ...
    set ddns-sn {string}
    set ddns-ttl {integer}
    set ddns-username {string}
    set ddns-zone {string}
    set monitor-interface <interface-name1>, <interface-name2>, ...
    set server-type [ipv4|ipv6]
    set ssl-certificate {string}
    set update-interval {integer}
    set use-public-ip [disable|enable]
  next
end
```

## config system ddns

Parameter	Description	Type	Size	Default
addr-type	Address type of interface address in DDNS update.	option	-	ipv4
bound-ip	Bound IP address.	string	Maximum length: 46	
clear-text	Enable/disable use of clear text connections.	option	-	disable
ddns-auth	Enable/disable TSIG authentication for your DDNS server.	option	-	disable

Parameter	Description	Type	Size	Default																								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable DDNS authentication.</td></tr><tr><td><i>tsig</i></td><td>Enable TSIG authentication based on RFC2845.</td></tr></table>				Option	Description	<i>disable</i>	Disable DDNS authentication.	<i>tsig</i>	Enable TSIG authentication based on RFC2845.																		
	Option	Description																										
	<i>disable</i>	Disable DDNS authentication.																										
<i>tsig</i>	Enable TSIG authentication based on RFC2845.																											
ddns-domain	Your fully qualified domain name. For example, yourname.ddns.com.	string	Maximum length: 64																									
ddns-key	DDNS update key (base 64 encoding).	password_aes256	Not Specified																									
ddns-keyname	DDNS update key name.	string	Maximum length: 64																									
ddns-password	DDNS password.	password	Not Specified																									
ddns-server	Select a DDNS service provider.	option	-																									
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>dyndns.org</i></td><td>members.dyndns.org and dnsalias.com</td></tr><tr><td><i>dyns.net</i></td><td>www.dyns.net</td></tr><tr><td><i>tzo.com</i></td><td>rh.tzo.com</td></tr><tr><td><i>vavic.com</i></td><td>Peanut Hull</td></tr><tr><td><i>dipdns.net</i></td><td>dipdnsserver.dipdns.com</td></tr><tr><td><i>now.net.cn</i></td><td>ip.todayisp.com</td></tr><tr><td><i>dhs.org</i></td><td>members.dhs.org</td></tr><tr><td><i>easydns.com</i></td><td>members.easydns.com</td></tr><tr><td><i>genericDDNS</i></td><td>Generic DDNS based on RFC2136.</td></tr><tr><td><i>FortiGuardDDNS</i></td><td>FortiGuard DDNS service.</td></tr><tr><td><i>noip.com</i></td><td>dynupdate.no-ip.com</td></tr></table>				Option	Description	<i>dyndns.org</i>	members.dyndns.org and dnsalias.com	<i>dyns.net</i>	www.dyns.net	<i>tzo.com</i>	rh.tzo.com	<i>vavic.com</i>	Peanut Hull	<i>dipdns.net</i>	dipdnsserver.dipdns.com	<i>now.net.cn</i>	ip.todayisp.com	<i>dhs.org</i>	members.dhs.org	<i>easydns.com</i>	members.easydns.com	<i>genericDDNS</i>	Generic DDNS based on RFC2136.	<i>FortiGuardDDNS</i>	FortiGuard DDNS service.	<i>noip.com</i>	dynupdate.no-ip.com
	Option	Description																										
	<i>dyndns.org</i>	members.dyndns.org and dnsalias.com																										
	<i>dyns.net</i>	www.dyns.net																										
	<i>tzo.com</i>	rh.tzo.com																										
	<i>vavic.com</i>	Peanut Hull																										
	<i>dipdns.net</i>	dipdnsserver.dipdns.com																										
	<i>now.net.cn</i>	ip.todayisp.com																										
	<i>dhs.org</i>	members.dhs.org																										
	<i>easydns.com</i>	members.easydns.com																										
	<i>genericDDNS</i>	Generic DDNS based on RFC2136.																										
	<i>FortiGuardDDNS</i>	FortiGuard DDNS service.																										
<i>noip.com</i>	dynupdate.no-ip.com																											
ddns-server-addr <addr>	Generic DDNS server IP/FQDN list. IP address or FQDN of the server.	string	Maximum length: 256																									
ddns-sn	DDNS Serial Number.	string	Maximum length: 64																									
ddns-ttl	Time-to-live for DDNS packets.	integer	Minimum value: 60 Maximum value: 86400	300																								

Parameter	Description	Type	Size	Default						
ddns-username	DDNS user name.	string	Maximum length: 64							
ddns-zone	Zone of your domain name (for example, DDNS.com).	string	Maximum length: 64							
ddnsid	DDNS ID.	integer	Minimum value: 0 Maximum value: 4294967295	0						
monitor-interface <interface-name>	Monitored interface. Interface name.	string	Maximum length: 79							
server-type	Address type of the DDNS server.	option	-	ipv4						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ipv4</td><td>Use IPv4 addressing.</td></tr><tr><td>ipv6</td><td>Use IPv6 addressing.</td></tr></table>				Option	Description	ipv4	Use IPv4 addressing.	ipv6	Use IPv6 addressing.
Option	Description									
ipv4	Use IPv4 addressing.									
ipv6	Use IPv6 addressing.									
ssl-certificate	Name of local certificate for SSL connections.	string	Maximum length: 35	Fortinet_Factory						
update-interval	DDNS update interval.	integer	Minimum value: 60 Maximum value: 2592000	0						
use-public-ip	Enable/disable use of public IP address.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable use of public IP address.</td></tr><tr><td>enable</td><td>Enable use of public IP address.</td></tr></table>				Option	Description	disable	Disable use of public IP address.	enable	Enable use of public IP address.
Option	Description									
disable	Disable use of public IP address.									
enable	Enable use of public IP address.									

## config system dedicated-mgmt

Configure dedicated management.

```
config system dedicated-mgmt
  Description: Configure dedicated management.
  set default-gateway {ipv4-address}
  set dhcp-end-ip {ipv4-address}
  set dhcp-netmask {ipv4-netmask}
  set dhcp-server [enable|disable]
  set dhcp-start-ip {ipv4-address}
  set interface {string}
```

```

    set status [enable|disable]
end

```

## config system dedicated-mgmt

Parameter	Description	Type	Size	Default
default-gateway	Default gateway for dedicated management interface.	ipv4-address	Not Specified	0.0.0.0
dhcp-end-ip	DHCP end IP for dedicated management.	ipv4-address	Not Specified	0.0.0.0
dhcp-netmask	DHCP netmask.	ipv4-netmask	Not Specified	0.0.0.0
dhcp-server	Enable/disable DHCP server on management interface.	option	-	disable
	<b>Option</b>		<b>Description</b>	
	<i>enable</i>		Enable DHCP server on management port.	
	<i>disable</i>		Disable DHCP server on management port.	
dhcp-start-ip	DHCP start IP for dedicated management.	ipv4-address	Not Specified	0.0.0.0
interface	Dedicated management interface.	string	Maximum length: 15	
status	Enable/disable dedicated management.	option	-	disable
	<b>Option</b>		<b>Description</b>	
	<i>enable</i>		Enable setting.	
	<i>disable</i>		Disable setting.	

## config system dhcp6 server

Configure DHCPv6 servers.

```

config system dhcp6 server
    Description: Configure DHCPv6 servers.
    edit <id>
        set delegated-prefix-iaid {integer}
        set dns-search-list [delegated|specify]
        set dns-server1 {ipv6-address}
        set dns-server2 {ipv6-address}
        set dns-server3 {ipv6-address}
        set dns-server4 {ipv6-address}
        set dns-service [delegated|default|...]
        set domain {string}
        set interface {string}
    end
end

```

```

set ip-mode [range|delegated]
config ip-range
    Description: DHCP IP range configuration.
    edit <id>
        set start-ip {ipv6-address}
        set end-ip {ipv6-address}
    next
end
set lease-time {integer}
set option1 {user}
set option2 {user}
set option3 {user}
set prefix-mode [dhcp6|ra]
config prefix-range
    Description: DHCP prefix configuration.
    edit <id>
        set start-prefix {ipv6-address}
        set end-prefix {ipv6-address}
        set prefix-length {integer}
    next
end
set rapid-commit [disable|enable]
set status [disable|enable]
set subnet {ipv6-prefix}
set upstream-interface {string}
next
end

```

## config system dhcp6 server

Parameter	Description	Type	Size	Default						
delegated-prefix-iaid	IAID of obtained delegated-prefix from the upstream interface.	integer	Minimum value: 0 Maximum value: 4294967295	0						
dns-search-list	DNS search list options.	option	-	specify						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>delegated</i></td><td>Delegated the DNS search list.</td></tr><tr><td><i>specify</i></td><td>Specify the DNS search list.</td></tr></table>				Option	Description	<i>delegated</i>	Delegated the DNS search list.	<i>specify</i>	Specify the DNS search list.
	Option	Description								
	<i>delegated</i>	Delegated the DNS search list.								
<i>specify</i>	Specify the DNS search list.									
dns-server1	DNS server 1.	ipv6-address	Not Specified	::						
dns-server2	DNS server 2.	ipv6-address	Not Specified	::						
dns-server3	DNS server 3.	ipv6-address	Not Specified	::						



Parameter	Description	Type	Size	Default
dns-server4	DNS server 4.	ipv6-address	Not Specified	::
dns-service	Options for assigning DNS servers to DHCPv6 clients.	option	-	specify
	<b>Option</b>		<b>Description</b>	
	<i>delegated</i>		Delegated DNS settings.	
	<i>default</i>		Clients are assigned the FortiGate's configured DNS servers.	
	<i>specify</i>		Specify up to 3 DNS servers in the DHCPv6 server configuration.	
domain	Domain name suffix for the IP addresses that the DHCP server assigns to clients.	string	Maximum length: 35	
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
interface	DHCP server can assign IP configurations to clients connected to this interface.	string	Maximum length: 15	
ip-mode	Method used to assign client IP.	option	-	range
	<b>Option</b>		<b>Description</b>	
	<i>range</i>		Use range defined by start IP/end IP to assign client IP.	
	<i>delegated</i>		Use delegated prefix method to assign client IP.	
lease-time	Lease time in seconds, 0 means unlimited.	integer	Minimum value: 300 Maximum value: 8640000	604800
option1	Option 1.	user	Not Specified	
option2	Option 2.	user	Not Specified	
option3	Option 3.	user	Not Specified	
prefix-mode	Assigning a prefix from a DHCPv6 client or RA.	option	-	dhcp6
	<b>Option</b>		<b>Description</b>	
	<i>dhcp6</i>		Use delegated prefix from a DHCPv6 client.	
	<i>ra</i>		Use prefix from RA.	
rapid-commit	Enable/disable allow/disallow rapid commit.	option	-	disable

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Do not allow rapid commit.		
	<i>enable</i>	Allow rapid commit.		
status	Enable/disable this DHCPv6 configuration.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Enable this DHCPv6 server configuration.		
	<i>enable</i>	Disable this DHCPv6 server configuration.		
subnet	Subnet or subnet-id if the IP mode is delegated.	ipv6-prefix	Not Specified	::/0
upstream-interface	Interface name from where delegated information is provided.	string	Maximum length: 15	

### config ip-range

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
start-ip	Start of IP range.	ipv6-address	Not Specified	::
end-ip	End of IP range.	ipv6-address	Not Specified	::

### config prefix-range

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
start-prefix	Start of prefix range.	ipv6-address	Not Specified	::
end-prefix	End of prefix range.	ipv6-address	Not Specified	::

Parameter	Description	Type	Size	Default
prefix-length	Prefix length.	integer	Minimum value: 1 Maximum value: 128	0

## config system dhcp server

Configure DHCP servers.

```

config system dhcp server
    Description: Configure DHCP servers.
    edit <id>
        set auto-configuration [disable|enable]
        set auto-managed-status [disable|enable]
        set conflicted-ip-timeout {integer}
        set ddns-auth [disable|tsig]
        set ddns-key {password_aes256}
        set ddns-keyname {string}
        set ddns-server-ip {ipv4-address}
        set ddns-ttl {integer}
        set ddns-update [disable|enable]
        set ddns-update-override [disable|enable]
        set ddns-zone {string}
        set default-gateway {ipv4-address}
        set dhcp-settings-from-fortiipam [disable|enable]
        set dns-server1 {ipv4-address}
        set dns-server2 {ipv4-address}
        set dns-server3 {ipv4-address}
        set dns-server4 {ipv4-address}
        set dns-service [local|default|...]
        set domain {string}
    config exclude-range
        Description: Exclude one or more ranges of IP addresses from being assigned to
clients.
        edit <id>
            set start-ip {ipv4-address}
            set end-ip {ipv4-address}
        next
    end
    set filename {string}
    set forticlient-on-net-status [disable|enable]
    set interface {string}
    set ip-mode [range|usrgrp]
    config ip-range
        Description: DHCP IP range configuration.
        edit <id>
            set start-ip {ipv4-address}
            set end-ip {ipv4-address}
        next
    end
    set ipsec-lease-hold {integer}
    set lease-time {integer}

```

```

set mac-acl-default-action [assign|block]
set netmask {ipv4-netmask}
set next-server {ipv4-address}
set ntp-server1 {ipv4-address}
set ntp-server2 {ipv4-address}
set ntp-server3 {ipv4-address}
set ntp-service [local|default|...]
config options
    Description: DHCP options.
    edit <id>
        set code {integer}
        set type [hex|string|...]
        set value {string}
        set ip {user}
    next
end
config reserved-address
    Description: Options for the DHCP server to assign IP settings to specific MAC
addresses.
    edit <id>
        set type [mac|option82]
        set ip {ipv4-address}
        set mac {mac-address}
        set action [assign|block|...]
        set circuit-id-type [hex|string]
        set circuit-id {string}
        set remote-id-type [hex|string]
        set remote-id {string}
        set description {var-string}
    next
end
set server-type [regular|ipsec]
set status [disable|enable]
set tftp-server <tftp-server1>, <tftp-server2>, ...
set timezone [01|02|...]
set timezone-option [disable|default|...]
set vci-match [disable|enable]
set vci-string <vci-string1>, <vci-string2>, ...
set wifi-ac-service [specify|local]
set wifi-ac1 {ipv4-address}
set wifi-ac2 {ipv4-address}
set wifi-ac3 {ipv4-address}
set wins-server1 {ipv4-address}
set wins-server2 {ipv4-address}
next
end

```

## config system dhcp server

Parameter	Description	Type	Size	Default
auto-configuration	Enable/disable auto configuration.	option	-	enable

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable auto configuration.</td></tr><tr><td><i>enable</i></td><td>Enable auto configuration.</td></tr></table>	Option	Description	<i>disable</i>	Disable auto configuration.	<i>enable</i>	Enable auto configuration.			
Option	Description									
<i>disable</i>	Disable auto configuration.									
<i>enable</i>	Enable auto configuration.									
auto-managed-status	Enable/disable use of this DHCP server once this interface has been assigned an IP address from FortiPAM.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable use of this DHCP server once this interface has been assigned an IP address from FortiPAM.</td></tr><tr><td><i>enable</i></td><td>Enable use of this DHCP server once this interface has been assigned an IP address from FortiPAM.</td></tr></table>	Option	Description	<i>disable</i>	Disable use of this DHCP server once this interface has been assigned an IP address from FortiPAM.	<i>enable</i>	Enable use of this DHCP server once this interface has been assigned an IP address from FortiPAM.			
Option	Description									
<i>disable</i>	Disable use of this DHCP server once this interface has been assigned an IP address from FortiPAM.									
<i>enable</i>	Enable use of this DHCP server once this interface has been assigned an IP address from FortiPAM.									
conflicted-ip-timeout	Time in seconds to wait after a conflicted IP address is removed from the DHCP range before it can be reused.	integer	Minimum value: 60 Maximum value: 8640000	1800						
ddns-auth	DDNS authentication mode.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable DDNS authentication.</td></tr><tr><td><i>tsig</i></td><td>TSIG based on RFC2845.</td></tr></table>	Option	Description	<i>disable</i>	Disable DDNS authentication.	<i>tsig</i>	TSIG based on RFC2845.			
Option	Description									
<i>disable</i>	Disable DDNS authentication.									
<i>tsig</i>	TSIG based on RFC2845.									
ddns-key	DDNS update key (base 64 encoding).	password_aes256	Not Specified							
ddns-keyname	DDNS update key name.	string	Maximum length: 64							
ddns-server-ip	DDNS server IP.	ipv4-address	Not Specified	0.0.0.0						
ddns-ttl	TTL.	integer	Minimum value: 60 Maximum value: 86400	300						
ddns-update	Enable/disable DDNS update for DHCP.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable DDNS update for DHCP.</td></tr><tr><td><i>enable</i></td><td>Enable DDNS update for DHCP.</td></tr></table>	Option	Description	<i>disable</i>	Disable DDNS update for DHCP.	<i>enable</i>	Enable DDNS update for DHCP.			
Option	Description									
<i>disable</i>	Disable DDNS update for DHCP.									
<i>enable</i>	Enable DDNS update for DHCP.									

Parameter	Description	Type	Size	Default
ddns-update-override	Enable/disable DDNS update override for DHCP.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable DDNS update override for DHCP.		
	<i>enable</i>	Enable DDNS update override for DHCP.		
ddns-zone	Zone of your domain name (ex. DDNS.com).	string	Maximum length: 64	
default-gateway	Default gateway IP address assigned by the DHCP server.	ipv4-address	Not Specified	0.0.0.0
dhcp-settings-from-fortiipam	Enable/disable populating of DHCP server settings from FortiPAM.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable populating of DHCP server settings from FortiPAM.		
	<i>enable</i>	Enable populating of DHCP server settings from FortiPAM.		
dns-server1	DNS server 1.	ipv4-address	Not Specified	0.0.0.0
dns-server2	DNS server 2.	ipv4-address	Not Specified	0.0.0.0
dns-server3	DNS server 3.	ipv4-address	Not Specified	0.0.0.0
dns-server4	DNS server 4.	ipv4-address	Not Specified	0.0.0.0
dns-service	Options for assigning DNS servers to DHCP clients.	option	-	specify
	<b>Option</b>	<b>Description</b>		
	<i>local</i>	IP address of the interface the DHCP server is added to becomes the client's DNS server IP address.		
	<i>default</i>	Clients are assigned the FortiGate's configured DNS servers.		
	<i>specify</i>	Specify up to 3 DNS servers in the DHCP server configuration.		
domain	Domain name suffix for the IP addresses that the DHCP server assigns to clients.	string	Maximum length: 35	
filename	Name of the boot file on the TFTP server.	string	Maximum length: 127	
forticlient-on-net-status	Enable/disable FortiClient-On-Net service for this DHCP server.	option	-	enable

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable FortiClient On-Net Status.		
	<i>enable</i>	Enable FortiClient On-Net Status.		
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
interface	DHCP server can assign IP configurations to clients connected to this interface.	string	Maximum length: 15	
ip-mode	Method used to assign client IP.	option	-	range
	<b>Option</b>	<b>Description</b>		
	<i>range</i>	Use range defined by start-ip/end-ip to assign client IP.		
	<i>usrgrp</i>	Use user-group defined method to assign client IP.		
ipsec-lease-hold	DHCP over IPsec leases expire this many seconds after tunnel down (0 to disable forced-expiry).	integer	Minimum value: 0 Maximum value: 8640000	60
lease-time	Lease time in seconds, 0 means unlimited.	integer	Minimum value: 300 Maximum value: 8640000	604800
mac-acl-default-action	MAC access control default action (allow or block assigning IP settings).	option	-	assign
	<b>Option</b>	<b>Description</b>		
	<i>assign</i>	Allow the DHCP server to assign IP settings to clients on the MAC access control list.		
	<i>block</i>	Block the DHCP server from assigning IP settings to clients on the MAC access control list.		
netmask	Netmask assigned by the DHCP server.	ipv4-netmask	Not Specified	0.0.0.0
next-server	IP address of a server (for example, a TFTP sever) that DHCP clients can download a boot file from.	ipv4-address	Not Specified	0.0.0.0
ntp-server1	NTP server 1.	ipv4-address	Not Specified	0.0.0.0

Parameter	Description	Type	Size	Default
ntp-server2	NTP server 2.	ipv4-address	Not Specified	0.0.0.0
ntp-server3	NTP server 3.	ipv4-address	Not Specified	0.0.0.0
ntp-service	Options for assigning Network Time Protocol (NTP) servers to DHCP clients.	option	-	specify
	<b>Option</b> <b>Description</b>			
	local	IP address of the interface the DHCP server is added to becomes the client's NTP server IP address.		
	default	Clients are assigned the FortiGate's configured NTP servers.		
	specify	Specify up to 3 NTP servers in the DHCP server configuration.		
server-type	DHCP server can be a normal DHCP server or an IPsec DHCP server.	option	-	regular
	<b>Option</b> <b>Description</b>			
	regular	Regular DHCP service.		
	ipsec	DHCP over IPsec service.		
status	Enable/disable this DHCP configuration.	option	-	enable
	<b>Option</b> <b>Description</b>			
	disable	Do not use this DHCP server configuration.		
	enable	Use this DHCP server configuration.		
tftp-server <tftp-server>	One or more hostnames or IP addresses of the TFTP servers in quotes separated by spaces. TFTP server.	string	Maximum length: 63	
timezone	Select the time zone to be assigned to DHCP clients.	option	-	00
	<b>Option</b> <b>Description</b>			
	01	(GMT-11:00) Midway Island, Samoa		
	02	(GMT-10:00) Hawaii		
	03	(GMT-9:00) Alaska		
	04	(GMT-8:00) Pacific Time (US & Canada)		
	05	(GMT-7:00) Arizona		
	81	(GMT-7:00) Baja California Sur, Chihuahua		
	06	(GMT-7:00) Mountain Time (US & Canada)		



Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	07	(GMT-6:00) Central America		
	08	(GMT-6:00) Central Time (US & Canada)		
	09	(GMT-6:00) Mexico City		
	10	(GMT-6:00) Saskatchewan		
	11	(GMT-5:00) Bogota, Lima, Quito		
	12	(GMT-5:00) Eastern Time (US & Canada)		
	13	(GMT-5:00) Indiana (East)		
	74	(GMT-4:00) Caracas		
	14	(GMT-4:00) Atlantic Time (Canada)		
	77	(GMT-4:00) Georgetown		
	15	(GMT-4:00) La Paz		
	87	(GMT-4:00) Paraguay		
	16	(GMT-3:00) Santiago		
	17	(GMT-3:30) Newfoundland		
	18	(GMT-3:00) Brasilia		
	19	(GMT-3:00) Buenos Aires		
	20	(GMT-3:00) Nuuk (Greenland)		
	75	(GMT-3:00) Uruguay		
	21	(GMT-2:00) Mid-Atlantic		
	22	(GMT-1:00) Azores		
	23	(GMT-1:00) Cape Verde Is.		
	24	(GMT) Monrovia		
	80	(GMT) Greenwich Mean Time		
	79	(GMT) Casablanca		
	25	(GMT) Dublin, Edinburgh, Lisbon, London, Canary Is.		
	26	(GMT+1:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna		
	27	(GMT+1:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague		
	28	(GMT+1:00) Brussels, Copenhagen, Madrid, Paris		
	78	(GMT+1:00) Namibia		

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	29	(GMT+1:00) Sarajevo, Skopje, Warsaw, Zagreb		
	30	(GMT+1:00) West Central Africa		
	31	(GMT+2:00) Athens, Sofia, Vilnius		
	32	(GMT+2:00) Bucharest		
	33	(GMT+2:00) Cairo		
	34	(GMT+2:00) Harare, Pretoria		
	35	(GMT+2:00) Helsinki, Riga, Tallinn		
	36	(GMT+2:00) Jerusalem		
	37	(GMT+3:00) Baghdad		
	38	(GMT+3:00) Kuwait, Riyadh		
	83	(GMT+3:00) Moscow		
	84	(GMT+3:00) Minsk		
	40	(GMT+3:00) Nairobi		
	85	(GMT+3:00) Istanbul		
	41	(GMT+3:30) Tehran		
	42	(GMT+4:00) Abu Dhabi, Muscat		
	43	(GMT+4:00) Baku		
	39	(GMT+3:00) St. Petersburg, Volgograd		
	44	(GMT+4:30) Kabul		
	46	(GMT+5:00) Islamabad, Karachi, Tashkent		
	47	(GMT+5:30) Kolkata, Chennai, Mumbai, New Delhi		
	51	(GMT+5:30) Sri Jayawardenepara		
	48	(GMT+5:45) Kathmandu		
	45	(GMT+5:00) Ekaterinburg		
	49	(GMT+6:00) Almaty, Novosibirsk		
	50	(GMT+6:00) Astana, Dhaka		
	52	(GMT+6:30) Rangoon		
	53	(GMT+7:00) Bangkok, Hanoi, Jakarta		
	54	(GMT+7:00) Krasnoyarsk		

Parameter	Description	Type	Size	Default																																																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>55</td><td>(GMT+8:00) Beijing, ChongQing, HongKong, Urumgi, Irkutsk</td></tr><tr><td>56</td><td>(GMT+8:00) Ulaan Bataar</td></tr><tr><td>57</td><td>(GMT+8:00) Kuala Lumpur, Singapore</td></tr><tr><td>58</td><td>(GMT+8:00) Perth</td></tr><tr><td>59</td><td>(GMT+8:00) Taipei</td></tr><tr><td>60</td><td>(GMT+9:00) Osaka, Sapporo, Tokyo, Seoul</td></tr><tr><td>62</td><td>(GMT+9:30) Adelaide</td></tr><tr><td>63</td><td>(GMT+9:30) Darwin</td></tr><tr><td>61</td><td>(GMT+9:00) Yakutsk</td></tr><tr><td>64</td><td>(GMT+10:00) Brisbane</td></tr><tr><td>65</td><td>(GMT+10:00) Canberra, Melbourne, Sydney</td></tr><tr><td>66</td><td>(GMT+10:00) Guam, Port Moresby</td></tr><tr><td>67</td><td>(GMT+10:00) Hobart</td></tr><tr><td>68</td><td>(GMT+10:00) Vladivostok</td></tr><tr><td>69</td><td>(GMT+10:00) Magadan</td></tr><tr><td>70</td><td>(GMT+11:00) Solomon Is., New Caledonia</td></tr><tr><td>71</td><td>(GMT+12:00) Auckland, Wellington</td></tr><tr><td>72</td><td>(GMT+12:00) Fiji, Kamchatka, Marshall Is.</td></tr><tr><td>00</td><td>(GMT+12:00) Eniwetok, Kwajalein</td></tr><tr><td>82</td><td>(GMT+12:45) Chatham Islands</td></tr><tr><td>73</td><td>(GMT+13:00) Nuku'alofa</td></tr><tr><td>86</td><td>(GMT+13:00) Samoa</td></tr><tr><td>76</td><td>(GMT+14:00) Kiritimati</td></tr></table>	Option	Description	55	(GMT+8:00) Beijing, ChongQing, HongKong, Urumgi, Irkutsk	56	(GMT+8:00) Ulaan Bataar	57	(GMT+8:00) Kuala Lumpur, Singapore	58	(GMT+8:00) Perth	59	(GMT+8:00) Taipei	60	(GMT+9:00) Osaka, Sapporo, Tokyo, Seoul	62	(GMT+9:30) Adelaide	63	(GMT+9:30) Darwin	61	(GMT+9:00) Yakutsk	64	(GMT+10:00) Brisbane	65	(GMT+10:00) Canberra, Melbourne, Sydney	66	(GMT+10:00) Guam, Port Moresby	67	(GMT+10:00) Hobart	68	(GMT+10:00) Vladivostok	69	(GMT+10:00) Magadan	70	(GMT+11:00) Solomon Is., New Caledonia	71	(GMT+12:00) Auckland, Wellington	72	(GMT+12:00) Fiji, Kamchatka, Marshall Is.	00	(GMT+12:00) Eniwetok, Kwajalein	82	(GMT+12:45) Chatham Islands	73	(GMT+13:00) Nuku'alofa	86	(GMT+13:00) Samoa	76	(GMT+14:00) Kiritimati			
	Option	Description																																																		
	55	(GMT+8:00) Beijing, ChongQing, HongKong, Urumgi, Irkutsk																																																		
	56	(GMT+8:00) Ulaan Bataar																																																		
	57	(GMT+8:00) Kuala Lumpur, Singapore																																																		
	58	(GMT+8:00) Perth																																																		
	59	(GMT+8:00) Taipei																																																		
	60	(GMT+9:00) Osaka, Sapporo, Tokyo, Seoul																																																		
	62	(GMT+9:30) Adelaide																																																		
	63	(GMT+9:30) Darwin																																																		
	61	(GMT+9:00) Yakutsk																																																		
	64	(GMT+10:00) Brisbane																																																		
	65	(GMT+10:00) Canberra, Melbourne, Sydney																																																		
	66	(GMT+10:00) Guam, Port Moresby																																																		
	67	(GMT+10:00) Hobart																																																		
	68	(GMT+10:00) Vladivostok																																																		
	69	(GMT+10:00) Magadan																																																		
	70	(GMT+11:00) Solomon Is., New Caledonia																																																		
	71	(GMT+12:00) Auckland, Wellington																																																		
	72	(GMT+12:00) Fiji, Kamchatka, Marshall Is.																																																		
	00	(GMT+12:00) Eniwetok, Kwajalein																																																		
	82	(GMT+12:45) Chatham Islands																																																		
	73	(GMT+13:00) Nuku'alofa																																																		
86	(GMT+13:00) Samoa																																																			
76	(GMT+14:00) Kiritimati																																																			
timezone-option	Options for the DHCP server to set the client's time zone.	option	-	disable																																																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Do not set the client's time zone.</td></tr><tr><td>default</td><td>Clients are assigned the FortiGate's configured time zone.</td></tr><tr><td>specify</td><td>Specify the time zone to be assigned to DHCP clients.</td></tr></table>	Option	Description	disable	Do not set the client's time zone.	default	Clients are assigned the FortiGate's configured time zone.	specify	Specify the time zone to be assigned to DHCP clients.																																											
	Option	Description																																																		
	disable	Do not set the client's time zone.																																																		
	default	Clients are assigned the FortiGate's configured time zone.																																																		
specify	Specify the time zone to be assigned to DHCP clients.																																																			

Parameter	Description	Type	Size	Default						
vci-match	Enable/disable vendor class identifier (VCI) matching. When enabled only DHCP requests with a matching VCI are served.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable VCI matching.</td></tr><tr><td><i>enable</i></td><td>Enable VCI matching.</td></tr></table>	Option	Description	<i>disable</i>	Disable VCI matching.	<i>enable</i>	Enable VCI matching.			
Option	Description									
<i>disable</i>	Disable VCI matching.									
<i>enable</i>	Enable VCI matching.									
vci-string <vci-string>	One or more VCI strings in quotes separated by spaces. VCI strings.	string	Maximum length: 255							
wifi-ac-service	Options for assigning WiFi access controllers to DHCP clients.	option	-	specify						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>specify</i></td><td>Specify up to 3 WiFi Access Controllers in the DHCP server configuration.</td></tr><tr><td><i>local</i></td><td>IP address of the interface the DHCP server is added to becomes the client's WiFi Access Controller IP address.</td></tr></table>	Option	Description	<i>specify</i>	Specify up to 3 WiFi Access Controllers in the DHCP server configuration.	<i>local</i>	IP address of the interface the DHCP server is added to becomes the client's WiFi Access Controller IP address.			
Option	Description									
<i>specify</i>	Specify up to 3 WiFi Access Controllers in the DHCP server configuration.									
<i>local</i>	IP address of the interface the DHCP server is added to becomes the client's WiFi Access Controller IP address.									
wifi-ac1	WiFi Access Controller 1 IP address (DHCP option 138, RFC 5417).	ipv4-address	Not Specified	0.0.0.0						
wifi-ac2	WiFi Access Controller 2 IP address (DHCP option 138, RFC 5417).	ipv4-address	Not Specified	0.0.0.0						
wifi-ac3	WiFi Access Controller 3 IP address (DHCP option 138, RFC 5417).	ipv4-address	Not Specified	0.0.0.0						
wins-server1	WINS server 1.	ipv4-address	Not Specified	0.0.0.0						
wins-server2	WINS server 2.	ipv4-address	Not Specified	0.0.0.0						

### config exclude-range

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
start-ip	Start of IP range.	ipv4-address	Not Specified	0.0.0.0
end-ip	End of IP range.	ipv4-address	Not Specified	0.0.0.0

## config ip-range

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
start-ip	Start of IP range.	ipv4-address	Not Specified	0.0.0.0
end-ip	End of IP range.	ipv4-address	Not Specified	0.0.0.0

## config options

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
code	DHCP option code.	integer	Minimum value: 0 Maximum value: 255	0
type	DHCP option type.	option	-	hex
	<b>Option</b>	<b>Description</b>		
	<i>hex</i>	DHCP option in hex.		
	<i>string</i>	DHCP option in string.		
	<i>ip</i>	DHCP option in IP.		
	<i>fqdn</i>	DHCP option in domain search option format.		
value	DHCP option value.	string	Maximum length: 312	
ip	DHCP option IPs.	user	Not Specified	

## config reserved-address

Parameter	Description	Type	Size	Default								
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0								
type	DHCP reserved-address type.	option	-	mac								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>mac</td><td>Match with MAC address.</td></tr><tr><td>option82</td><td>Match with DHCP option 82.</td></tr></table>	Option	Description	mac	Match with MAC address.	option82	Match with DHCP option 82.					
Option	Description											
mac	Match with MAC address.											
option82	Match with DHCP option 82.											
ip	IP address to be reserved for the MAC address.	ipv4-address	Not Specified	0.0.0.0								
mac	MAC address of the client that will get the reserved IP address.	mac-address	Not Specified	00:00:00:00:00:00								
action	Options for the DHCP server to configure the client with the reserved MAC address.	option	-	reserved								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>assign</td><td>Configure the client with this MAC address like any other client.</td></tr><tr><td>block</td><td>Block the DHCP server from assigning IP settings to the client with this MAC address.</td></tr><tr><td>reserved</td><td>Assign the reserved IP address to the client with this MAC address.</td></tr></table>	Option	Description	assign	Configure the client with this MAC address like any other client.	block	Block the DHCP server from assigning IP settings to the client with this MAC address.	reserved	Assign the reserved IP address to the client with this MAC address.			
Option	Description											
assign	Configure the client with this MAC address like any other client.											
block	Block the DHCP server from assigning IP settings to the client with this MAC address.											
reserved	Assign the reserved IP address to the client with this MAC address.											
circuit-id-type	DHCP option type.	option	-	string								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>hex</td><td>DHCP option in hex.</td></tr><tr><td>string</td><td>DHCP option in string.</td></tr></table>	Option	Description	hex	DHCP option in hex.	string	DHCP option in string.					
Option	Description											
hex	DHCP option in hex.											
string	DHCP option in string.											
circuit-id	Option 82 circuit-ID of the client that will get the reserved IP address.	string	Maximum length: 312									
remote-id-type	DHCP option type.	option	-	string								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>hex</td><td>DHCP option in hex.</td></tr><tr><td>string</td><td>DHCP option in string.</td></tr></table>	Option	Description	hex	DHCP option in hex.	string	DHCP option in string.					
Option	Description											
hex	DHCP option in hex.											
string	DHCP option in string.											

Parameter	Description	Type	Size	Default
remote-id	Option 82 remote-ID of the client that will get the reserved IP address.	string	Maximum length: 312	
description	Description.	var-string	Maximum length: 255	

## config system dnp3-proxy



This command is available for model(s): FortiGateRugged 60F 3G4G, FortiGateRugged 60F. It is not available for: FortiGate 1000D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate VM64, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

Configure dnpproxy settings.

```
config system dnp3-proxy
    Description: Configure dnpproxysettings.
    set port {integer}
    set status [enable|disable]
    set term-baudrate [19200|38400|...]
    set term-databits {integer}
    set term-flowcontrol [none|xon_xoff|...]
    set term-parity [none|odd|...]
    set term-stopbits {integer}
end
```

## config system dnp3-proxy

Parameter	Description	Type	Size	Default								
port	DNP3 TCPServer Port.	integer	Minimum value: 1 Maximum value: 65535	20000								
status	Enable/disable DNP daemon.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable DNP daemon.</td></tr><tr><td><i>disable</i></td><td>Disable DNP daemon.</td></tr></table>	Option	Description	<i>enable</i>	Enable DNP daemon.	<i>disable</i>	Disable DNP daemon.					
Option	Description											
<i>enable</i>	Enable DNP daemon.											
<i>disable</i>	Disable DNP daemon.											
term-baudrate	Term Baudrate.	option	-	19200								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>19200</i></td><td>set DNP baudrate to 19200</td></tr><tr><td><i>38400</i></td><td>set DNP baudrate to 38400</td></tr><tr><td><i>115200</i></td><td>set DNP baudrate to 115200</td></tr></table>	Option	Description	<i>19200</i>	set DNP baudrate to 19200	<i>38400</i>	set DNP baudrate to 38400	<i>115200</i>	set DNP baudrate to 115200			
Option	Description											
<i>19200</i>	set DNP baudrate to 19200											
<i>38400</i>	set DNP baudrate to 38400											
<i>115200</i>	set DNP baudrate to 115200											
term-databits	Term Data Bits.	integer	Minimum value: 0 Maximum value: 65535	8								
term-flowcontrol	Term Flow Control	option	-	none								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>No flow control.</td></tr><tr><td><i>xon_xoff</i></td><td>Enable software flow control on both input and output.</td></tr><tr><td><i>hardware</i></td><td>Enable hardware flow control.</td></tr></table>	Option	Description	<i>none</i>	No flow control.	<i>xon_xoff</i>	Enable software flow control on both input and output.	<i>hardware</i>	Enable hardware flow control.			
Option	Description											
<i>none</i>	No flow control.											
<i>xon_xoff</i>	Enable software flow control on both input and output.											
<i>hardware</i>	Enable hardware flow control.											
term-parity	Term Parity	option	-	none								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>No parity check.</td></tr><tr><td><i>odd</i></td><td>Odd parity check.</td></tr><tr><td><i>even</i></td><td>Even parity check.</td></tr></table>	Option	Description	<i>none</i>	No parity check.	<i>odd</i>	Odd parity check.	<i>even</i>	Even parity check.			
Option	Description											
<i>none</i>	No parity check.											
<i>odd</i>	Odd parity check.											
<i>even</i>	Even parity check.											



Parameter	Description	Type	Size	Default
term-stopbits	Term Stop Bits.	integer	Minimum value: 0 Maximum value: 65535	1

## config system dns-database

Configure DNS databases.

```

config system dns-database
    Description: Configure DNS databases.
    edit <name>
        set allow-transfer {user}
        set authoritative [enable|disable]
        set contact {string}
    config dns-entry
        Description: DNS entry.
        edit <id>
            set status [enable|disable]
            set type [A|NS|...]
            set ttl {integer}
            set preference {integer}
            set ip {ipv4-address-any}
            set ipv6 {ipv6-address}
            set hostname {string}
            set canonical-name {string}
        next
    end
    set domain {string}
    set forwarder {user}
    set ip-primary {ipv4-address-any}
    set primary-name {string}
    set rr-max {integer}
    set source-ip {ipv4-address}
    set status [enable|disable]
    set ttl {integer}
    set type [primary|secondary]
    set view [shadow|public]
next
end

```

## config system dns-database

Parameter	Description	Type	Size	Default
allow-transfer	DNS zone transfer IP address list.	user	Not Specified	
authoritative	Enable/disable authoritative zone.	option	-	enable

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable authoritative zone.</td></tr><tr><td><i>disable</i></td><td>Disable authoritative zone.</td></tr></table>	Option	Description	<i>enable</i>	Enable authoritative zone.	<i>disable</i>	Disable authoritative zone.			
	Option	Description								
	<i>enable</i>	Enable authoritative zone.								
<i>disable</i>	Disable authoritative zone.									
contact	Email address of the administrator for this zone. You can specify only the username, such as admin or the full email address, such as admin@test.com When using only a username, the domain of the email will be this zone.	string	Maximum length: 255	host						
domain	Domain name.	string	Maximum length: 255							
forwarder	DNS zone forwarder IP address list.	user	Not Specified							
ip-primary	IP address of primary DNS server. Entries in this primary DNS server and imported into the DNS zone.	ipv4-address-any	Not Specified	0.0.0.0						
name	Zone name.	string	Maximum length: 35							
primary-name	Domain name of the default DNS server for this zone.	string	Maximum length: 255	dns						
rr-max	Maximum number of resource records.	integer	Minimum value: 10 Maximum value: 65536	16384						
source-ip	Source IP for forwarding to DNS server.	ipv4-address	Not Specified	0.0.0.0						
status	Enable/disable this DNS zone.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
	Option	Description								
	<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.									
ttl	Default time-to-live value for the entries of this DNS zone.	integer	Minimum value: 0 Maximum value: 2147483647	86400						
type	Zone type (primary to manage entries directly, secondary to import entries from other zones).	option	-	primary						

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>primary</i>	Primary DNS zone, to manage entries directly.		
	<i>secondary</i>	Secondary DNS zone, to import entries from other DNS zones.		
view	Zone view (public to serve public clients, shadow to serve internal clients).	option	-	shadow
	<b>Option</b>	<b>Description</b>		
	<i>shadow</i>	Shadow DNS zone to serve internal clients.		
	<i>public</i>	Public DNS zone to serve public clients.		

### config dns-entry

Parameter	Description	Type	Size	Default
id	DNS entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
status	Enable/disable resource record status.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable resource record status.		
	<i>disable</i>	Disable resource record status.		
type	Resource record type.	option	-	A
	<b>Option</b>	<b>Description</b>		
	<i>A</i>	Host type.		
	<i>NS</i>	Name server type.		
	<i>CNAME</i>	Canonical name type.		
	<i>MX</i>	Mail exchange type.		
	<i>AAAA</i>	IPv6 host type.		
	<i>PTR</i>	Pointer type.		
	<i>PTR_V6</i>	IPv6 pointer type.		

Parameter	Description	Type	Size	Default
ttl	Time-to-live for this entry.	integer	Minimum value: 0 Maximum value: 2147483647	0
preference	DNS entry preference.	integer	Minimum value: 0 Maximum value: 65535	10
ip	IPv4 address of the host.	ipv4-address-any	Not Specified	0.0.0.0
ipv6	IPv6 address of the host.	ipv6-address	Not Specified	::
hostname	Name of the host.	string	Maximum length: 255	
canonical-name	Canonical name of the host.	string	Maximum length: 255	

## config system dns-server

Configure DNS servers.

```
config system dns-server
    Description: Configure DNS servers.
    edit <name>
        set dnsfilter-profile {string}
        set doh [enable|disable]
        set mode [recursive|non-recursive|...]
    next
end
```

## config system dns-server

Parameter	Description	Type	Size	Default
dnsfilter-profile	DNS filter profile.	string	Maximum length: 35	
doh	DNS over HTTPS/443.	option	-	disable
		Option	Description	
		<i>enable</i>	Enable DNS over HTTPS.	

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable DNS over HTTPS.		
mode	DNS server mode.	option	-	recursive
	<b>Option</b>	<b>Description</b>		
	<i>recursive</i>	Shadow DNS database and forward.		
	<i>non-recursive</i>	Public DNS database only.		
	<i>forward-only</i>	Forward only.		
name	DNS server name.	string	Maximum length: 15	

## config system dns

Configure DNS.

```
config system dns
    Description: Configure DNS.
    set alt-primary {ipv4-address}
    set alt-secondary {ipv4-address}
    set cache-notfound-responses [disable|enable]
    set dns-cache-limit {integer}
    set dns-cache-ttl {integer}
    set domain <domain1>, <domain2>, ...
    set interface {string}
    set interface-select-method [auto|sdwan|...]
    set ip6-primary {ipv6-address}
    set ip6-secondary {ipv6-address}
    set log [disable|error|...]
    set primary {ipv4-address}
    set protocol {option1}, {option2}, ...
    set retry {integer}
    set secondary {ipv4-address}
    set server-hostname <hostname1>, <hostname2>, ...
    set server-select-method [least-rtt|failover]
    set source-ip {ipv4-address}
    set ssl-certificate {string}
    set timeout {integer}
end
```

## config system dns

Parameter	Description	Type	Size	Default
alt-primary	Alternate primary DNS server. This is not used as a failover DNS server.	ipv4-address	Not Specified	0.0.0.0

Parameter	Description	Type	Size	Default								
alt-secondary	Alternate secondary DNS server. This is not used as a failover DNS server.	ipv4-address	Not Specified	0.0.0.0								
cache-notfound-responses	Enable/disable response from the DNS server when a record is not in cache.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable cache NOTFOUND responses from DNS server.</td></tr><tr><td><i>enable</i></td><td>Enable cache NOTFOUND responses from DNS server.</td></tr></table>				Option	Description	<i>disable</i>	Disable cache NOTFOUND responses from DNS server.	<i>enable</i>	Enable cache NOTFOUND responses from DNS server.		
Option	Description											
<i>disable</i>	Disable cache NOTFOUND responses from DNS server.											
<i>enable</i>	Enable cache NOTFOUND responses from DNS server.											
dns-cache-limit	Maximum number of records in the DNS cache.	integer	Minimum value: 0 Maximum value: 4294967295	5000								
dns-cache-ttl	Duration in seconds that the DNS cache retains information.	integer	Minimum value: 60 Maximum value: 86400	1800								
domain <domain>	Search suffix list for hostname lookup. DNS search domain list separated by space (maximum 8 domains).	string	Maximum length: 127									
interface	Specify outgoing interface to reach server.	string	Maximum length: 15									
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto</i></td><td>Set outgoing interface automatically.</td></tr><tr><td><i>sdwan</i></td><td>Set outgoing interface by SD-WAN or policy routing rules.</td></tr><tr><td><i>specify</i></td><td>Set outgoing interface manually.</td></tr></table>				Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.
Option	Description											
<i>auto</i>	Set outgoing interface automatically.											
<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.											
<i>specify</i>	Set outgoing interface manually.											
ip6-primary	Primary DNS server IPv6 address.	ipv6-address	Not Specified	::								
ip6-secondary	Secondary DNS server IPv6 address.	ipv6-address	Not Specified	::								
log	Local DNS log setting.	option	-	disable								

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable.		
	<i>error</i>	Enable local DNS error log.		
	<i>all</i>	Enable local DNS log.		
primary	Primary DNS server IP address.	ipv4-address	Not Specified	0.0.0.0
protocol	DNS transport protocols.	option	-	cleartext
	<b>Option</b>	<b>Description</b>		
	<i>cleartext</i>	DNS over UDP/53, DNS over TCP/53.		
	<i>dot</i>	DNS over TLS/853.		
	<i>doh</i>	DNS over HTTPS/443.		
retry	Number of times to retry.	integer	Minimum value: 0 Maximum value: 5	2
secondary	Secondary DNS server IP address.	ipv4-address	Not Specified	0.0.0.0
server-hostname <hostname>	DNS server host name list. DNS server host name list separated by space (maximum 4 domains).	string	Maximum length: 127	
server-select-method	Specify how configured servers are prioritized.	option	-	least-rtt
	<b>Option</b>	<b>Description</b>		
	<i>least-rtt</i>	Select servers based on least round trip time.		
	<i>failover</i>	Select servers based on the order they are configured.		
source-ip	IP address used by the DNS server as its source IP.	ipv4-address	Not Specified	0.0.0.0
ssl-certificate	Name of local certificate for SSL connections.	string	Maximum length: 35	Fortinet_Factory
timeout	DNS query timeout interval in seconds.	integer	Minimum value: 1 Maximum value: 10	5

## config system dns64

Configure DNS64.

```
config system dns64
    Description: Configure DNS64.
    set always-synthesize-aaaa-record [enable|disable]
    set dns64-prefix {ipv6-prefix}
    set status [enable|disable]
end
```

## config system dns64

Parameter	Description	Type	Size	Default
always-synthesize-aaaa-record	Enable/disable AAAA record synthesis.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable AAAA record synthesis.		
	<i>disable</i>	Disable AAAA record synthesis.		
dns64-prefix	DNS64 prefix must be ::/96.	ipv6-prefix	Not Specified	64:ff9b::/96
status	Enable/disable DNS64.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable DNS64.		
	<i>disable</i>	Disable DNS64.		

## config system dscp-based-priority

Configure DSCP based priority table.

```
config system dscp-based-priority
    Description: Configure DSCP based priority table.
    edit <id>
        set ds {integer}
        set priority [low|medium|...]
    next
end
```



## config system dscp-based-priority

Parameter	Description	Type	Size	Default
ds	DSCP.	integer	Minimum value: 0 Maximum value: 63	0
id	Item ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
priority	DSCP based priority level.	option	-	high
	Option	Description		
	low	Low priority.		
	medium	Medium priority.		
	high	High priority.		

## config system elbc



This command is available for model(s): FortiGate 5001E1, FortiGate 5001E.

It is not available for: FortiGate 1000D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

Configure enhanced load balance cluster.

```

config system elbc
    Description: Configure enhanced load balance cluster.
    set graceful-upgrade [enable|disable]
    set hb-device <name1>, <name2>, ...
    set inter-chassis-support [enable|disable]
    set mode [none|forticontroller|...]
end

```

## config system elbc

Parameter	Description	Type	Size	Default								
graceful-upgrade	enable/disable graceful upgrade	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
hb-device <name>	ELBC heartbeat device. set interface name	string	Maximum length: 79									
inter-chassis-support	Enable/disable content-cluster across multiple chassis.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable content-cluster across multiple chassis.</td></tr><tr><td><i>disable</i></td><td>Disable content-cluster across multiple chassis.</td></tr></table>	Option	Description	<i>enable</i>	Enable content-cluster across multiple chassis.	<i>disable</i>	Disable content-cluster across multiple chassis.					
Option	Description											
<i>enable</i>	Enable content-cluster across multiple chassis.											
<i>disable</i>	Disable content-cluster across multiple chassis.											
mode	ELBC mode.	option	-	none								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>ELBC mode disabled.</td></tr><tr><td><i>forticontroller</i></td><td>FortiController.</td></tr><tr><td><i>dual-forticontroller</i></td><td>Dual-FortiController.</td></tr></table>	Option	Description	<i>none</i>	ELBC mode disabled.	<i>forticontroller</i>	FortiController.	<i>dual-forticontroller</i>	Dual-FortiController.			
Option	Description											
<i>none</i>	ELBC mode disabled.											
<i>forticontroller</i>	FortiController.											
<i>dual-forticontroller</i>	Dual-FortiController.											

## config system email-server

Configure the email server used by the FortiGate various things. For example, for sending email messages to users to support user authentication features.

```

config system email-server
    Description: Configure the email server used by the FortiGate various things. For
example, for sending email messages to users to support user authentication features.
    set authenticate [enable|disable]
    set interface {string}

```

```

set interface-select-method [auto|sdwan|...]
set password {password}
set port {integer}
set reply-to {string}
set security [none|starttls|...]
set server {string}
set source-ip {ipv4-address}
set source-ip6 {ipv6-address}
set ssl-min-proto-version [default|SSLv3|...]
set type {option}
set username {string}
set validate-server [enable|disable]
end

```

## config system email-server

Parameter	Description	Type	Size	Default								
authenticate	Enable/disable authentication.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable authentication.</td></tr><tr><td><i>disable</i></td><td>Disable authentication.</td></tr></table>	Option	Description	<i>enable</i>	Enable authentication.	<i>disable</i>	Disable authentication.					
Option	Description											
<i>enable</i>	Enable authentication.											
<i>disable</i>	Disable authentication.											
interface	Specify outgoing interface to reach server.	string	Maximum length: 15									
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto</i></td><td>Set outgoing interface automatically.</td></tr><tr><td><i>sdwan</i></td><td>Set outgoing interface by SD-WAN or policy routing rules.</td></tr><tr><td><i>specify</i></td><td>Set outgoing interface manually.</td></tr></table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.			
Option	Description											
<i>auto</i>	Set outgoing interface automatically.											
<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.											
<i>specify</i>	Set outgoing interface manually.											
password	SMTP server user password for authentication.	password	Not Specified									
port	SMTP server port.	integer	Minimum value: 1 Maximum value: 65535	25								
reply-to	Reply-To email address.	string	Maximum length: 63									
security	Connection security used by the email server.	option	-	none								

Parameter	Description	Type	Size	Default												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>None.</td></tr><tr><td><i>starttls</i></td><td>STARTTLS.</td></tr><tr><td><i>smtps</i></td><td>SSL/TLS.</td></tr></table>				Option	Description	<i>none</i>	None.	<i>starttls</i>	STARTTLS.	<i>smtps</i>	SSL/TLS.				
	Option	Description														
	<i>none</i>	None.														
	<i>starttls</i>	STARTTLS.														
<i>smtps</i>	SSL/TLS.															
server	SMTP server IP address or hostname.	string	Maximum length: 63													
source-ip	SMTP server IPv4 source IP.	ipv4-address	Not Specified	0.0.0.0												
source-ip6	SMTP server IPv6 source IP.	ipv6-address	Not Specified	::												
ssl-min-protocol-version	Minimum supported protocol version for SSL/TLS connections.	option	-	default												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>Follow system global setting.</td></tr><tr><td><i>SSLv3</i></td><td>SSLv3.</td></tr><tr><td><i>TLSv1</i></td><td>TLSv1.</td></tr><tr><td><i>TLSv1-1</i></td><td>TLSv1.1.</td></tr><tr><td><i>TLSv1-2</i></td><td>TLSv1.2.</td></tr></table>				Option	Description	<i>default</i>	Follow system global setting.	<i>SSLv3</i>	SSLv3.	<i>TLSv1</i>	TLSv1.	<i>TLSv1-1</i>	TLSv1.1.	<i>TLSv1-2</i>	TLSv1.2.
	Option	Description														
	<i>default</i>	Follow system global setting.														
	<i>SSLv3</i>	SSLv3.														
	<i>TLSv1</i>	TLSv1.														
	<i>TLSv1-1</i>	TLSv1.1.														
<i>TLSv1-2</i>	TLSv1.2.															
type	Use FortiGuard Message service or custom email server.	option	-	custom												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>custom</i></td><td>Use custom email server.</td></tr></table>				Option	Description	<i>custom</i>	Use custom email server.								
	Option	Description														
<i>custom</i>	Use custom email server.															
username	SMTP server user name for authentication.	string	Maximum length: 63													
validate-server	Enable/disable validation of server certificate.	option	-	disable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable validation of server certificate.</td></tr><tr><td><i>disable</i></td><td>Disable validation of server certificate.</td></tr></table>				Option	Description	<i>enable</i>	Enable validation of server certificate.	<i>disable</i>	Disable validation of server certificate.						
	Option	Description														
	<i>enable</i>	Enable validation of server certificate.														
<i>disable</i>	Disable validation of server certificate.															

## config system external-resource

Configure external resource.

```

config system external-resource
    Description: Configure external resource.
    edit <name>
        set category {integer}
        set comments {var-string}
        set interface {string}
        set interface-select-method [auto|sdwan|...]
        set password {password}
        set refresh-rate {integer}
        set resource {string}
        set server-identity-check [none|basic|...]
        set source-ip {ipv4-address}
        set status [enable|disable]
        set type [category|address|...]
        set user-agent {var-string}
        set username {string}
        set uuid {uuid}
    next
end

```

## config system external-resource

Parameter	Description	Type	Size	Default								
category	User resource category.	integer	Minimum value: 192 Maximum value: 221	0								
comments	Comment.	var-string	Maximum length: 255									
interface	Specify outgoing interface to reach server.	string	Maximum length: 15									
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto</i></td><td>Set outgoing interface automatically.</td></tr><tr><td><i>sdwan</i></td><td>Set outgoing interface by SD-WAN or policy routing rules.</td></tr><tr><td><i>specify</i></td><td>Set outgoing interface manually.</td></tr></table>				Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.
	Option	Description										
	<i>auto</i>	Set outgoing interface automatically.										
	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.										
<i>specify</i>	Set outgoing interface manually.											
name	External resource name.	string	Maximum length: 35									
password	HTTP basic authentication password.	password	Not Specified									

Parameter	Description	Type	Size	Default										
refresh-rate	Time interval to refresh external resource.	integer	Minimum value: 1 Maximum value: 43200	5										
resource	URI of external resource.	string	Maximum length: 511											
server-identity-check	Certificate verification option.	option	-	none										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>No certificate verification.</td></tr><tr><td><i>basic</i></td><td>Check server certificate only.</td></tr><tr><td><i>full</i></td><td>Check server certificate and verify the domain matches in the server certificate.</td></tr></table>				Option	Description	<i>none</i>	No certificate verification.	<i>basic</i>	Check server certificate only.	<i>full</i>	Check server certificate and verify the domain matches in the server certificate.		
Option	Description													
<i>none</i>	No certificate verification.													
<i>basic</i>	Check server certificate only.													
<i>full</i>	Check server certificate and verify the domain matches in the server certificate.													
source-ip	Source IPv4 address used to communicate with server.	ipv4-address	Not Specified	0.0.0.0										
status	Enable/disable user resource.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable user resource.</td></tr><tr><td><i>disable</i></td><td>Disable user resource.</td></tr></table>				Option	Description	<i>enable</i>	Enable user resource.	<i>disable</i>	Disable user resource.				
Option	Description													
<i>enable</i>	Enable user resource.													
<i>disable</i>	Disable user resource.													
type	User resource type.	option	-	category										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>category</i></td><td>FortiGuard category.</td></tr><tr><td><i>address</i></td><td>Firewall IP address.</td></tr><tr><td><i>domain</i></td><td>Domain Name.</td></tr><tr><td><i>malware</i></td><td>Malware hash.</td></tr></table>				Option	Description	<i>category</i>	FortiGuard category.	<i>address</i>	Firewall IP address.	<i>domain</i>	Domain Name.	<i>malware</i>	Malware hash.
Option	Description													
<i>category</i>	FortiGuard category.													
<i>address</i>	Firewall IP address.													
<i>domain</i>	Domain Name.													
<i>malware</i>	Malware hash.													
user-agent	HTTP User-Agent header.	var-string	Maximum length: 255											
username	HTTP basic authentication user name.	string	Maximum length: 64											
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000										

## config system federated-upgrade

Coordinate federated upgrades within the Security Fabric.

```
config system federated-upgrade
  Description: Coordinate federated upgrades within the Security Fabric.
  set failure-device {string}
  set failure-reason [none|internal|...]
  set next-path-index {integer}
  config node-list
    Description: Nodes which will be included in the upgrade.
    edit <serial>
      set timing [immediate|scheduled]
      set time {user}
      set setup-time {user}
      set upgrade-path {user}
      set device-type [fortigate|fortiswitch|...]
      set coordinating-fortigate {string}
    next
  end
  set status [disabled|initialized|...]
  set upgrade-id {integer}
end
```

## config system federated-upgrade

Parameter	Description	Type	Size	Default
failure-device	Serial number of the node to include.	string	Maximum length: 79	
failure-reason	Reason for upgrade failure.	option	-	none
		Option	Description	
		<i>none</i>	No failure.	
		<i>internal</i>	An internal error occurred.	
		<i>timeout</i>	The upgrade timed out.	
		<i>device-type-unsupported</i>	The device type was not supported by the FortiGate.	
		<i>download-failed</i>	The image could not be downloaded.	
		<i>device-missing</i>	The device was disconnected from the FortiGate.	
		<i>version-unavailable</i>	An image matching the device and version could not be found.	
		<i>staging-failed</i>	The image could not be pushed to the device.	
		<i>reboot-failed</i>	The device could not be rebooted.	

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>device-not-reconnected</i>	The device did not reconnect after rebooting.		
	<i>node-not-ready</i>	A device in the CSF tree was not ready.		
	<i>no-final-confirmation</i>	The coordinating FortiGate did not confirm the upgrade.		
	<i>no-confirmation-query</i>	A downstream FortiGate did not initiate final confirmation.		
next-path-index	The index of the next image to upgrade to.	integer	Minimum value: 0 Maximum value: 10	0
status	Current status of the upgrade.	option	-	disabled
	<b>Option</b>	<b>Description</b>		
	<i>disabled</i>	No federated upgrade has been configured.		
	<i>initialized</i>	The upgrade has been configured.		
	<i>downloading</i>	The image is downloading in preparation for the upgrade.		
	<i>device-disconnected</i>	The image downloads are complete, but one or more devices have disconnected.		
	<i>ready</i>	The image download finished and the upgrade is pending.		
	<i>staging</i>	The upgrade is confirmed and images are being staged.		
	<i>final-check</i>	The upgrade is ready and final checks are in progress.		
	<i>upgrade-devices</i>	The upgrade is ready and devices are being rebooted.		
	<i>cancelled</i>	The upgrade was cancelled due to the tree not being ready.		
	<i>confirmed</i>	The upgrade was confirmed and reboots are running.		
	<i>done</i>	The upgrade completed successfully.		
	<i>failed</i>	The upgrade failed due to a local issue.		
upgrade-id	Unique identifier for this upgrade.	integer	Minimum value: 0 Maximum value: 4294967295	0



## config node-list

Parameter	Description	Type	Size	Default
serial	Serial number of the node to include.	string	Maximum length: 79	
timing	Whether the upgrade should be run immediately, or at a scheduled time.	option	-	immediate
	<b>Option</b>	<b>Description</b>		
	<i>immediate</i>	Begin the upgrade immediately.		
	<i>scheduled</i>	Begin the upgrade at a configured time.		
time	Scheduled time for the upgrade. Format hh:mm yyyy/mm/dd UTC.	user	Not Specified	
setup-time	When the upgrade was configured. Format hh:mm yyyy/mm/dd UTC.	user	Not Specified	
upgrade-path	Image IDs to upgrade through.	user	Not Specified	
device-type	What type of device this node represents.	option	-	fortigate
	<b>Option</b>	<b>Description</b>		
	<i>fortigate</i>	This device is a FortiGate.		
	<i>fortiswitch</i>	This device is a FortiSwitch.		
	<i>fortiap</i>	This device is a FortiAP.		
coordinating-fortigate	Serial number of the FortiGate unit that controls this device.	string	Maximum length: 79	

## config system fips-cc

Configure FIPS-CC mode.

```
config system fips-cc
  Description: Configure FIPS-CC mode.
  set entropy-token [enable|disable|...]
  set key-generation-self-test [enable|disable]
  set self-test-period {integer}
  set status [enable|disable]
end
```

## config system fips-cc

Parameter	Description	Type	Size	Default
entropy-token	Enable/disable/dynamic entropy token.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable entropy token to be present during boot process.		
	<i>disable</i>	Disable entropy token to be present during boot process.		
	<i>dynamic</i>	Dynamic detect entropy token to be present during boot process.		
key-generation-self-test	Enable/disable self tests after key generation.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable self tests after key generation.		
	<i>disable</i>	Disable self tests after key generation.		
self-test-period	Self test period.	integer	Minimum value: 1 Maximum value: 1440	1440
status	Enable/disable ciphers for FIPS mode of operation.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable FIPS-CC mode.		
	<i>disable</i>	Disable FIPS-CC mode.		

## config system fortiguard

Configure FortiGuard services.

```
config system fortiguard
  Description: Configure FortiGuard services.
  set antispam-cache [enable|disable]
  set antispam-cache-mpercent {integer}
  set antispam-cache-ttl {integer}
  set antispam-expiration {integer}
  set antispam-force-off [enable|disable]
  set antispam-license {integer}
  set antispam-timeout {integer}
  set anycast-sdns-server-ip {ipv4-address}
  set anycast-sdns-server-port {integer}
  set auto-join-forticloud [enable|disable]
  set ddns-server-ip {ipv4-address}
```

```

set ddns-server-ip6 {ipv6-address}
set ddns-server-port {integer}
set fortiguard-anycast [enable|disable]
set fortiguard-anycast-source [fortinet|aws|...]
set interface {string}
set interface-select-method [auto|sdwan|...]
set load-balance-servers {integer}
set outbreak-prevention-cache [enable|disable]
set outbreak-prevention-cache-mpercent {integer}
set outbreak-prevention-cache-ttl {integer}
set outbreak-prevention-expiration {integer}
set outbreak-prevention-force-off [enable|disable]
set outbreak-prevention-license {integer}
set outbreak-prevention-timeout {integer}
set persistent-connection [enable|disable]
set port [8888|53|...]
set protocol [udp|http|...]
set proxy-password {password}
set proxy-server-ip {ipv4-address}
set proxy-server-port {integer}
set proxy-username {string}
set sandbox-region {string}
set sdns-options {option1}, {option2}, ...
set sdns-server-ip {user}
set sdns-server-port {integer}
set service-account-id {string}
set source-ip {ipv4-address}
set source-ip6 {ipv6-address}
set update-build-proxy [enable|disable]
set update-extdb [enable|disable]
set update-ffdb [enable|disable]
set update-server-location [automatic|usa|...]
set update-uwdb [enable|disable]
set videofilter-expiration {integer}
set videofilter-license {integer}
set webfilter-cache [enable|disable]
set webfilter-cache-ttl {integer}
set webfilter-expiration {integer}
set webfilter-force-off [enable|disable]
set webfilter-license {integer}
set webfilter-timeout {integer}
end

```

end

## config system fortiguard

Parameter	Description	Type	Size	Default
antispam-cache	Enable/disable FortiGuard antispam request caching. Uses a small amount of memory but improves performance.	option	-	enable

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable FortiGuard antispam request caching.		
	<i>disable</i>	Disable FortiGuard antispam request caching.		
antispam-cache-mpercent	Maximum percentage of FortiGate memory the antispam cache is allowed to use.	integer	Minimum value: 1 Maximum value: 15	2
antispam-cache-ttl	Time-to-live for antispam cache entries in seconds. Lower times reduce the cache size. Higher times may improve performance since the cache will have more entries.	integer	Minimum value: 300 Maximum value: 86400	1800
antispam-expiration	Expiration date of the FortiGuard antispam contract.	integer	Minimum value: 0 Maximum value: 4294967295	0
antispam-force-off	Enable/disable turning off the FortiGuard antispam service.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Turn off the FortiGuard antispam service.		
	<i>disable</i>	Allow the FortiGuard antispam service.		
antispam-license	Interval of time between license checks for the FortiGuard antispam contract.	integer	Minimum value: 0 Maximum value: 4294967295	4294967295
antispam-timeout	Antispam query time out.	integer	Minimum value: 1 Maximum value: 30	7
anycast-sdns-server-ip	IP address of the FortiGuard anycast DNS rating server.	ipv4-address	Not Specified	0.0.0.0
anycast-sdns-server-port	Port to connect to on the FortiGuard anycast DNS rating server.	integer	Minimum value: 1 Maximum value: 65535	853

Parameter	Description	Type	Size	Default
auto-join-forticloud *	Automatically connect to and login to FortiCloud.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable automatic connection and login to FortiCloud.		
	<i>disable</i>	Disable automatic connection and login to FortiCloud.		
ddns-server-ip	IP address of the FortiDDNS server.	ipv4-address	Not Specified	0.0.0.0
ddns-server-ip6	IPv6 address of the FortiDDNS server.	ipv6-address	Not Specified	::
ddns-server-port	Port used to communicate with FortiDDNS servers.	integer	Minimum value: 1 Maximum value: 65535	443
fortiguard-anycast	Enable/disable use of FortiGuard's Anycast network.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable use of FortiGuard's Anycast network.		
	<i>disable</i>	Disable use of FortiGuard's Anycast network.		
fortiguard-anycast-source	Configure which of Fortinet's servers to provide FortiGuard services in FortiGuard's anycast network. Default is Fortinet.	option	-	fortinet
	<b>Option</b>	<b>Description</b>		
	<i>fortinet</i>	Use Fortinet's servers to provide FortiGuard services in FortiGuard's anycast network.		
	<i>aws</i>	Use Fortinet's AWS servers to provide FortiGuard services in FortiGuard's anycast network.		
	<i>debug</i>	Use Fortinet's internal test servers to provide FortiGuard services in FortiGuard's anycast network.		
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto</i></td><td>Set outgoing interface automatically.</td></tr><tr><td><i>sdwan</i></td><td>Set outgoing interface by SD-WAN or policy routing rules.</td></tr><tr><td><i>specify</i></td><td>Set outgoing interface manually.</td></tr></table>				Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.
	Option	Description										
	<i>auto</i>	Set outgoing interface automatically.										
	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.										
<i>specify</i>	Set outgoing interface manually.											
load-balance-servers	Number of servers to alternate between as first FortiGuard option.	integer	Minimum value: 1 Maximum value: 266	1								
outbreak-prevention-cache	Enable/disable FortiGuard Virus Outbreak Prevention cache.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable FortiGuard antivirus caching.</td></tr><tr><td><i>disable</i></td><td>Disable FortiGuard antivirus caching.</td></tr></table>				Option	Description	<i>enable</i>	Enable FortiGuard antivirus caching.	<i>disable</i>	Disable FortiGuard antivirus caching.		
	Option	Description										
	<i>enable</i>	Enable FortiGuard antivirus caching.										
<i>disable</i>	Disable FortiGuard antivirus caching.											
outbreak-prevention-cache-mpercent	Maximum percent of memory FortiGuard Virus Outbreak Prevention cache can use.	integer	Minimum value: 1 Maximum value: 15	2								
outbreak-prevention-cache-ttl	Time-to-live for FortiGuard Virus Outbreak Prevention cache entries.	integer	Minimum value: 300 Maximum value: 86400	300								
outbreak-prevention-expiration	Expiration date of FortiGuard Virus Outbreak Prevention contract.	integer	Minimum value: 0 Maximum value: 4294967295	0								
outbreak-prevention-force-off	Turn off FortiGuard Virus Outbreak Prevention service.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Turn off FortiGuard antivirus service.</td></tr><tr><td><i>disable</i></td><td>Allow the FortiGuard antivirus service.</td></tr></table>				Option	Description	<i>enable</i>	Turn off FortiGuard antivirus service.	<i>disable</i>	Allow the FortiGuard antivirus service.		
	Option	Description										
	<i>enable</i>	Turn off FortiGuard antivirus service.										
<i>disable</i>	Allow the FortiGuard antivirus service.											

Parameter	Description	Type	Size	Default
outbreak-prevention-license	Interval of time between license checks for FortiGuard Virus Outbreak Prevention contract.	integer	Minimum value: 0 Maximum value: 4294967295	4294967295
outbreak-prevention-timeout	FortiGuard Virus Outbreak Prevention time out.	integer	Minimum value: 1 Maximum value: 30	7
persistent-connection	Enable/disable use of persistent connection to receive update notification from FortiGuard.	option	-	disable
	<b>Option</b>		<b>Description</b>	
	<i>enable</i>		Enable persistent connection to receive update notification from FortiGuard.	
	<i>disable</i>		Disable persistent connection to receive update notification from FortiGuard.	
port	Port used to communicate with the FortiGuard servers.	option	-	443
	<b>Option</b>		<b>Description</b>	
	<i>8888</i>		port 8888 for server communication.	
	<i>53</i>		port 53 for server communication.	
	<i>80</i>		port 80 for server communication.	
	<i>443</i>		port 443 for server communication.	
protocol	Protocol used to communicate with the FortiGuard servers.	option	-	https
	<b>Option</b>		<b>Description</b>	
	<i>udp</i>		UDP for server communication (for use by FortiGuard or FortiManager).	
	<i>http</i>		HTTP for server communication (for use only by FortiManager).	
	<i>https</i>		HTTPS for server communication (for use by FortiGuard or FortiManager).	
proxy-password	Proxy user password.	password	Not Specified	
proxy-server-ip	IP address of the proxy server.	ipv4-address	Not Specified	0.0.0.0

Parameter	Description	Type	Size	Default						
proxy-server-port	Port used to communicate with the proxy server.	integer	Minimum value: 0 Maximum value: 65535	0						
proxy-username	Proxy user name.	string	Maximum length: 64							
sandbox-region	Cloud sandbox region.	string	Maximum length: 63							
sdns-options	Customization options for the FortiGuard DNS service.	option	-							
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>include-question-section</i></td><td>Include DNS question section in the FortiGuard DNS setup message.</td></tr></table>				Option	Description	<i>include-question-section</i>	Include DNS question section in the FortiGuard DNS setup message.		
Option	Description									
<i>include-question-section</i>	Include DNS question section in the FortiGuard DNS setup message.									
sdns-server-ip	IP address of the FortiGuard DNS rating server.	user	Not Specified							
sdns-server-port	Port to connect to on the FortiGuard DNS rating server.	integer	Minimum value: 1 Maximum value: 65535	53						
service-account-id	Service account ID.	string	Maximum length: 50							
source-ip	Source IPv4 address used to communicate with FortiGuard.	ipv4-address	Not Specified	0.0.0.0						
source-ip6	Source IPv6 address used to communicate with FortiGuard.	ipv6-address	Not Specified	::						
update-build-proxy	Enable/disable proxy dictionary rebuild.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable proxy dictionary rebuild.</td></tr><tr><td><i>disable</i></td><td>Disable proxy dictionary rebuild.</td></tr></table>				Option	Description	<i>enable</i>	Enable proxy dictionary rebuild.	<i>disable</i>	Disable proxy dictionary rebuild.
Option	Description									
<i>enable</i>	Enable proxy dictionary rebuild.									
<i>disable</i>	Disable proxy dictionary rebuild.									
update-extdb	Enable/disable external resource update.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable external resource update.</td></tr><tr><td><i>disable</i></td><td>Disable external resource update.</td></tr></table>				Option	Description	<i>enable</i>	Enable external resource update.	<i>disable</i>	Disable external resource update.
Option	Description									
<i>enable</i>	Enable external resource update.									
<i>disable</i>	Disable external resource update.									



Parameter	Description	Type	Size	Default								
update-ffdb	Enable/disable Internet Service Database update.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Internet Service Database update.</td></tr><tr><td><i>disable</i></td><td>Disable Internet Service Database update.</td></tr></table>	Option	Description	<i>enable</i>	Enable Internet Service Database update.	<i>disable</i>	Disable Internet Service Database update.					
Option	Description											
<i>enable</i>	Enable Internet Service Database update.											
<i>disable</i>	Disable Internet Service Database update.											
update-server-location	Location from which to receive FortiGuard updates.	option	-	automatic								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>automatic</i></td><td>FortiGuard servers chosen based on closest proximity to FortiGate unit.</td></tr><tr><td><i>usa</i></td><td>FortiGuard servers in United States.</td></tr><tr><td><i>eu</i></td><td>FortiGuard servers in the European Union.</td></tr></table>	Option	Description	<i>automatic</i>	FortiGuard servers chosen based on closest proximity to FortiGate unit.	<i>usa</i>	FortiGuard servers in United States.	<i>eu</i>	FortiGuard servers in the European Union.			
Option	Description											
<i>automatic</i>	FortiGuard servers chosen based on closest proximity to FortiGate unit.											
<i>usa</i>	FortiGuard servers in United States.											
<i>eu</i>	FortiGuard servers in the European Union.											
update-uwdb	Enable/disable allowlist update.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable allowlist update.</td></tr><tr><td><i>disable</i></td><td>Disable allowlist update.</td></tr></table>	Option	Description	<i>enable</i>	Enable allowlist update.	<i>disable</i>	Disable allowlist update.					
Option	Description											
<i>enable</i>	Enable allowlist update.											
<i>disable</i>	Disable allowlist update.											
videofilter-expiration	Expiration date of the FortiGuard video filter contract.	integer	Minimum value: 0 Maximum value: 4294967295	0								
videofilter-license	Interval of time between license checks for the FortiGuard video filter contract.	integer	Minimum value: 0 Maximum value: 4294967295	4294967295								
webfilter-cache	Enable/disable FortiGuard web filter caching.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable FortiGuard web filter caching.</td></tr><tr><td><i>disable</i></td><td>Disable FortiGuard web filter caching.</td></tr></table>	Option	Description	<i>enable</i>	Enable FortiGuard web filter caching.	<i>disable</i>	Disable FortiGuard web filter caching.					
Option	Description											
<i>enable</i>	Enable FortiGuard web filter caching.											
<i>disable</i>	Disable FortiGuard web filter caching.											

Parameter	Description	Type	Size	Default						
webfilter-cache-ttl	Time-to-live for web filter cache entries in seconds.	integer	Minimum value: 300 Maximum value: 86400	3600						
webfilter-expiration	Expiration date of the FortiGuard web filter contract.	integer	Minimum value: 0 Maximum value: 4294967295	0						
webfilter-force-off	Enable/disable turning off the FortiGuard web filtering service.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Turn off the FortiGuard web filtering service.</td></tr><tr><td>disable</td><td>Allow the FortiGuard web filtering service to operate.</td></tr></table>				Option	Description	enable	Turn off the FortiGuard web filtering service.	disable	Allow the FortiGuard web filtering service to operate.
Option	Description									
enable	Turn off the FortiGuard web filtering service.									
disable	Allow the FortiGuard web filtering service to operate.									
webfilter-license	Interval of time between license checks for the FortiGuard web filter contract.	integer	Minimum value: 0 Maximum value: 4294967295	4294967295						
webfilter-timeout	Web filter query time out.	integer	Minimum value: 1 Maximum value: 30	15						

\* This parameter may not exist in some models.

## config system fortindr

Configure FortiNDR.

```

config system fortindr
    Description: Configure FortiNDR.
    set interface {string}
    set interface-select-method [auto|sdwan|...]
    set source-ip {string}
    set status [disable|enable]
end

```

## config system fortindr

Parameter	Description	Type	Size	Default
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto
	Option	Description		
	auto	Set outgoing interface automatically.		
	sdwan	Set outgoing interface by SD-WAN or policy routing rules.		
	specify	Set outgoing interface manually.		
source-ip	Source IP address for communications to FortiNDR.	string	Maximum length: 63	
status	Enable/disable FortiNDR.	option	-	disable
	Option	Description		
	disable	Disable FortiNDR.		
	enable	Enable FortiNDR.		

## config system fortisandbox

Configure FortiSandbox.

```
config system fortisandbox
  Description: Configure FortiSandbox.
  set email {string}
  set enc-algorithm [default|high|...]
  set forticloud [enable|disable]
  set interface {string}
  set interface-select-method [auto|sdwan|...]
  set server {string}
  set source-ip {string}
  set ssl-min-proto-version [default|SSLv3|...]
  set status [enable|disable]
end
```

## config system fortisandbox

Parameter	Description	Type	Size	Default
email	Notifier email address.	string	Maximum length: 63	

Parameter	Description	Type	Size	Default
enc-algorithm	Configure the level of SSL protection for secure communication with FortiSandbox.	option	-	default
	<b>Option</b>	<b>Description</b>		
	<i>default</i>	SSL communication with high and medium encryption algorithms.		
	<i>high</i>	SSL communication with high encryption algorithms.		
	<i>low</i>	SSL communication with low encryption algorithms.		
forticloud	Enable/disable FortiSandbox Cloud.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable FortiSandbox Cloud.		
	<i>disable</i>	Disable FortiSandbox Cloud.		
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto
	<b>Option</b>	<b>Description</b>		
	<i>auto</i>	Set outgoing interface automatically.		
	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.		
	<i>specify</i>	Set outgoing interface manually.		
server	Server address of the remote FortiSandbox.	string	Maximum length: 63	
source-ip	Source IP address for communications to FortiSandbox.	string	Maximum length: 63	
ssl-min-protocol-version	Minimum supported protocol version for SSL/TLS connections.	option	-	default
	<b>Option</b>	<b>Description</b>		
	<i>default</i>	Follow system global setting.		
	<i>SSLv3</i>	SSLv3.		
	<i>TLSv1</i>	TLSv1.		
	<i>TLSv1-1</i>	TLSv1.1.		
	<i>TLSv1-2</i>	TLSv1.2.		
status	Enable/disable FortiSandbox.	option	-	disable

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable FortiSandbox.		
	<i>disable</i>	Disable FortiSandbox.		

## config system fsso-polling

Configure Fortinet Single Sign On (FSSO) server.

```
config system fsso-polling
    Description: Configure Fortinet Single Sign On (FSSO) server.
    set auth-password {password}
    set authentication [enable|disable]
    set listening-port {integer}
    set status [enable|disable]
end
```

## config system fsso-polling

Parameter	Description	Type	Size	Default
auth-password	Password to connect to FSSO Agent.	password	Not Specified	
authentication	Enable/disable FSSO Agent Authentication.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable FSSO Agent Authentication.		
	<i>disable</i>	Disable FSSO Agent Authentication.		
listening-port	Listening port to accept clients.	integer	Minimum value: 1 Maximum value: 65535	8000
status	Enable/disable FSSO Polling Mode.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable FSSO Polling Mode.		
	<i>disable</i>	Disable FSSO Polling Mode.		

## config system ftm-push

Configure FortiToken Mobile push services.

```
config system ftm-push
  Description: Configure FortiToken Mobile push services.
  set server {string}
  set server-cert {string}
  set server-ip {ipv4-address}
  set server-port {integer}
  set status [enable|disable]
end
```

## config system ftm-push

Parameter	Description	Type	Size	Default
server	IPv4 address or domain name of FortiToken Mobile push services server.	string	Maximum length: 127	
server-cert	Name of the server certificate to be used for SSL.	string	Maximum length: 35	Fortinet_Factory
server-ip	IPv4 address of FortiToken Mobile push services server (format: xxx.xxx.xxx.xxx).	ipv4-address	Not Specified	0.0.0.0
server-port	Port to communicate with FortiToken Mobile push services server.	integer	Minimum value: 1 Maximum value: 65535	4433
status	Enable/disable the use of FortiToken Mobile push services.	option	-	disable
		Option	Description	
		<i>enable</i>	Enable FortiToken Mobile push services.	
		<i>disable</i>	Disable FortiToken Mobile push services.	

## config system geneve

Configure GENEVE devices.

```
config system geneve
  Description: Configure GENEVE devices.
  edit <name>
    set dstport {integer}
    set interface {string}
    set ip-version [ipv4-unicast|ipv6-unicast]
    set remote-ip {ipv4-address}
    set remote-ip6 {ipv6-address}
```

```

        set type [ethernet|ppp]
        set vni {integer}
    next
end

```

## config system geneve

Parameter	Description	Type	Size	Default						
dstport	GENEVE destination port.	integer	Minimum value: 1 Maximum value: 65535	6081						
interface	Outgoing interface for GENEVE encapsulated traffic.	string	Maximum length: 15							
ip-version	IP version to use for the GENEVE interface and so for communication over the GENEVE. IPv4 or IPv6 unicast.	option	-	ipv4-unicast						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ipv4-unicast</td><td>Use IPv4 unicast addressing over the GENEVE.</td></tr><tr><td>ipv6-unicast</td><td>Use IPv6 unicast addressing over the GENEVE.</td></tr></table>				Option	Description	ipv4-unicast	Use IPv4 unicast addressing over the GENEVE.	ipv6-unicast	Use IPv6 unicast addressing over the GENEVE.
Option	Description									
ipv4-unicast	Use IPv4 unicast addressing over the GENEVE.									
ipv6-unicast	Use IPv6 unicast addressing over the GENEVE.									
name	GENEVE device or interface name. Must be an unique interface name.	string	Maximum length: 15							
remote-ip	IPv4 address of the GENEVE interface on the device at the remote end of the GENEVE.	ipv4-address	Not Specified	0.0.0.0						
remote-ip6	IPv6 IP address of the GENEVE interface on the device at the remote end of the GENEVE.	ipv6-address	Not Specified	::						
type	GENEVE type.	option	-	ethernet						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ethernet</td><td>Internal packet includes Ethernet header.</td></tr><tr><td>ppp</td><td>Internal packet does not include Ethernet header.</td></tr></table>				Option	Description	ethernet	Internal packet includes Ethernet header.	ppp	Internal packet does not include Ethernet header.
Option	Description									
ethernet	Internal packet includes Ethernet header.									
ppp	Internal packet does not include Ethernet header.									
vni	GENEVE network ID.	integer	Minimum value: 0 Maximum value: 16777215	0						

## config system geoip-override

Configure geographical location mapping for IP address(es) to override mappings from FortiGuard.

```

config system geoip-override
    Description: Configure geographical location mapping for IP address(es) to override
    mappings from FortiGuard.
    edit <name>
        set country-id {string}
        set description {string}
        config ip-range
            Description: Table of IP ranges assigned to country.
            edit <id>
                set start-ip {ipv4-address}
                set end-ip {ipv4-address}
            next
        end
        config ip6-range
            Description: Table of IPv6 ranges assigned to country.
            edit <id>
                set start-ip {ipv6-address}
                set end-ip {ipv6-address}
            next
        end
    next
end

```

## config system geoip-override

Parameter	Description	Type	Size	Default
country-id	Two character Country ID code.	string	Maximum length: 2	
description	Description.	string	Maximum length: 127	
name	Location name.	string	Maximum length: 63	

## config ip-range

Parameter	Description	Type	Size	Default
id	ID of individual entry in the IP range table.	integer	Minimum value: 0 Maximum value: 65535	0
start-ip	Starting IP address, inclusive, of the address range (format: xxx.xxx.xxx.xxx).	ipv4-address	Not Specified	0.0.0.0
end-ip	Ending IP address, inclusive, of the address range (format: xxx.xxx.xxx.xxx).	ipv4-address	Not Specified	0.0.0.0



## config ip6-range

Parameter	Description	Type	Size	Default
id	ID of individual entry in the IPv6 range table.	integer	Minimum value: 0 Maximum value: 65535	0
start-ip	Starting IP address, inclusive, of the address range (format: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx).	ipv6-address	Not Specified	::
end-ip	Ending IP address, inclusive, of the address range (format: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx).	ipv6-address	Not Specified	::

## config system gi-gk



This command is available for model(s): FortiGate 2600F, FortiGate 3000F, FortiGate 3001F, FortiGate 3400E.

It is not available for: FortiGate 1000D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2601F, FortiGate 3000D, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

Configure Gi Firewall Gatekeeper.

```
config system gi-gk
    Description: Configure Gi Firewall Gatekeeper.
    set context {integer}
    set port {integer}
end
```

## config system gi-gk

Parameter	Description	Type	Size	Default
context	Context ID	integer	Minimum value: 0 Maximum value: 4294967295	696
port	UDP port to listen, range 0-65535.	integer	Minimum value: 0 Maximum value: 65535	21123

## config system global

Configure global attributes.

```
config system global
  Description: Configure global attributes.
  set admin-concurrent [enable|disable]
  set admin-console-timeout {integer}
  set admin-forticloud-sso-login [enable|disable]
  set admin-host {string}
  set admin-hsts-max-age {integer}
  set admin-https-pki-required [enable|disable]
  set admin-https-redirect [enable|disable]
  set admin-https-ssl-banned-ciphers {option1}, {option2}, ...
  set admin-https-ssl-ciphersuites {option1}, {option2}, ...
  set admin-https-ssl-versions {option1}, {option2}, ...
  set admin-lockout-duration {integer}
  set admin-lockout-threshold {integer}
  set admin-login-max {integer}
  set admin-maintainer [enable|disable]
  set admin-port {integer}
  set admin-reset-button [enable|disable]
  set admin-restrict-local [enable|disable]
  set admin-scp [enable|disable]
  set admin-server-cert {string}
  set admin-sport {integer}
  set admin-ssh-grace-time {integer}
  set admin-ssh-password [enable|disable]
  set admin-ssh-port {integer}
  set admin-ssh-v1 [enable|disable]
  set admin-telnet [enable|disable]
  set admin-telnet-port {integer}
  set admintimeout {integer}
  set alias {string}
  set allow-traffic-redirect [enable|disable]
  set anti-replay [disable|loose|...]
  set arp-max-entry {integer}
  set auth-cert {string}
```

---

```
set auth-http-port {integer}
set auth-https-port {integer}
set auth-keepalive [enable|disable]
set auth-session-limit [block-new|logout-inactive]
set auto-auth-extension-device [enable|disable]
set autorun-log-fsck [enable|disable]
set av-affinity {string}
set av-failopen [pass|off|...]
set av-failopen-session [enable|disable]
set batch-cmdb [enable|disable]
set block-session-timer {integer}
set br-fdb-max-entry {integer}
set cert-chain-max {integer}
set cfg-revert-timeout {integer}
set cfg-save [automatic|manual|...]
set check-protocol-header [loose|strict]
set check-reset-range [strict|disable]
set cli-audit-log [enable|disable]
set cloud-communication [enable|disable]
set clt-cert-req [enable|disable]
set cmdbsvr-affinity {string}
set cpu-use-threshold {integer}
set csr-ca-attribute [enable|disable]
set daily-restart [enable|disable]
set default-service-source-port {user}
set device-idle-timeout {integer}
set dh-params [1024|1536|...]
set dnsproxy-worker-count {integer}
set dst [enable|disable]
set early-tcp-npu-session [enable|disable]
set edit-vdom-prompt [enable|disable]
set extender-controller-reserved-network {ipv4-classnet-host}
set failtime {integer}
set faz-disk-buffer-size {integer}
set fds-statistics [enable|disable]
set fds-statistics-period {integer}
set fgd-alert-subscription {option1}, {option2}, ...
set forticarrier-bypass [enable|disable]
set forticontroller-proxy [enable|disable]
set forticontroller-proxy-port {integer}
set fortiextender [disable|enable]
set fortiextender-data-port {integer}
set fortiextender-discovery-lockdown [disable|enable]
set fortiextender-vlan-mode [enable|disable]
set fortiservice-port {integer}
set fortitoken-cloud [enable|disable]
set gui-allow-default-hostname [enable|disable]
set gui-allow-incompatible-fabric-fgt [enable|disable]
set gui-cdn-domain-override {string}
set gui-cdn-usage [enable|disable]
set gui-certificates [enable|disable]
set gui-custom-language [enable|disable]
set gui-date-format [yyyy/MM/dd|dd/MM/yyyy|...]
set gui-date-time-source [system|browser]
set gui-device-latitude {string}
set gui-device-longitude {string}
```

---

```
set gui-display-hostname [enable|disable]
set gui-firmware-upgrade-warning [enable|disable]
set gui-forticare-registration-setup-warning [enable|disable]
set gui-fortigate-cloud-sandbox [enable|disable]
set gui-fortiguard-resource-fetch [enable|disable]
set gui-ipv6 [enable|disable]
set gui-local-out [enable|disable]
set gui-replacement-message-groups [enable|disable]
set gui-rest-api-cache [enable|disable]
set gui-theme [jade|neutrino|...]
set gui-wireless-opensecurity [enable|disable]
set ha-affinity {string}
set honor-df [enable|disable]
set hostname {string}
set hyper-scale-vdom-num {integer}
set igmp-state-limit {integer}
set internal-switch-speed {option1}, {option2}, ...
set internet-service-database [mini|standard|...]
set interval {integer}
set ip-fragment-mem-thresholds {integer}
set ip-src-port-range {user}
set ips-affinity {string}
set ipsec-asic-offload [enable|disable]
set ipsec-ha-seqjump-rate {integer}
set ipsec-hmac-offload [enable|disable]
set ipsec-round-robin [enable|disable]
set ipsec-soft-dec-async [enable|disable]
set ipv6-accept-dad {integer}
set ipv6-allow-anycast-probe [enable|disable]
set ipv6-allow-local-in-silent-drop [enable|disable]
set ipv6-allow-multicast-probe [enable|disable]
set ipv6-allow-traffic-redirect [enable|disable]
set irq-time-accounting [auto|force]
set language [english|french|...]
set ldapconntimeout {integer}
set legacy-poe-device-support [enable|disable]
set lldp-reception [enable|disable]
set lldp-transmission [enable|disable]
set log-ssl-connection [enable|disable]
set log-uuid-address [enable|disable]
set login-timestamp [enable|disable]
set long-vdom-name [enable|disable]
set management-ip {string}
set management-port {integer}
set management-port-use-admin-sport [enable|disable]
set management-vdom {string}
set max-route-cache-size {integer}
set memory-use-threshold-extreme {integer}
set memory-use-threshold-green {integer}
set memory-use-threshold-red {integer}
set miglog-affinity {string}
set miglogd-children {integer}
set multi-factor-authentication [optional|mandatory]
set ndp-max-entry {integer}
set per-user-bal [enable|disable]
set pmtu-discovery [enable|disable]
```

```

set policy-auth-concurrent {integer}
set post-login-banner [disable|enable]
set pre-login-banner [enable|disable]
set private-data-encryption [disable|enable]
set proxy-auth-lifetime [enable|disable]
set proxy-auth-lifetime-timeout {integer}
set proxy-auth-timeout {integer}
set proxy-cert-use-mgmt-vdom [enable|disable]
set proxy-hardware-acceleration [disable|enable]
set proxy-re-authentication-mode [session|traffic|...]
set proxy-resource-mode [enable|disable]
set proxy-worker-count {integer}
set radius-port {integer}
set reboot-upon-config-restore [enable|disable]
set refresh {integer}
set remoteauthtimeout {integer}
set reset-sessionless-tcp [enable|disable]
set restart-time {user}
set revision-backup-on-logout [enable|disable]
set revision-image-auto-backup [enable|disable]
set scanunit-count {integer}
set security-rating-result-submission [enable|disable]
set security-rating-run-on-schedule [enable|disable]
set send-pmtu-icmp [enable|disable]
set show-backplane-intf [enable|disable]
set snat-route-change [enable|disable]
set special-file-23-support [disable|enable]
set speedtest-server [enable|disable]
set split-port {string}
config split-port-mode
    Description: Configure split port mode of ports.
    edit <interface>
        set split-mode [disable|4x10G|...]
    next
end
set ssd-trim-date {integer}
set ssd-trim-freq [never|hourly|...]
set ssd-trim-hour {integer}
set ssd-trim-min {integer}
set ssd-trim-weekday [sunday|monday|...]
set ssh-enc-algo {option1}, {option2}, ...
set ssh-kex-algo {option1}, {option2}, ...
set ssh-mac-algo {option1}, {option2}, ...
set ssl-min-proto-version [SSLv3|TLSv1|...]
set ssl-static-key-ciphers [enable|disable]
set sslvpn-cipher-hardware-acceleration [enable|disable]
set sslvpn-ems-sn-check [enable|disable]
set sslvpn-kxp-hardware-acceleration [enable|disable]
set sslvpn-max-worker-count {integer}
set sslvpn-plugin-version-check [enable|disable]
set strict-dirty-session-check [enable|disable]
set strong-crypto [enable|disable]
set switch-controller [disable|enable]
set switch-controller-reserved-network {ipv4-classnet-host}
set sys-perf-log-interval {integer}
set tcp-halfclose-timer {integer}

```

```

set tcp-halfopen-timer {integer}
set tcp-option [enable|disable]
set tcp-rst-timer {integer}
set tcp-timewait-timer {integer}
set tftp [enable|disable]
set timezone [01|02|...]
set traffic-priority [tos|dscp]
set traffic-priority-level [low|medium|...]
set two-factor-email-expiry {integer}
set two-factor-fac-expiry {integer}
set two-factor-ftk-expiry {integer}
set two-factor-ftm-expiry {integer}
set two-factor-sms-expiry {integer}
set udp-idle-timer {integer}
set url-filter-affinity {string}
set url-filter-count {integer}
set user-device-store-max-devices {integer}
set user-device-store-max-unified-mem {integer}
set user-device-store-max-users {integer}
set user-server-cert {string}
set vdom-mode [no-vdom|split-vdom|...]
set vip-arp-range [unlimited|restricted]
set virtual-switch-vlan [enable|disable]
set wad-affinity {string}
set wad-csvc-cs-count {integer}
set wad-csvc-db-count {integer}
set wad-memory-change-granularity {integer}
set wad-source-affinity [disable|enable]
set wad-worker-count {integer}
set wifi-ca-certificate {string}
set wifi-certificate {string}
set wimax-4g-usb [enable|disable]
set wireless-controller [enable|disable]
set wireless-controller-port {integer}
set wireless-mode [ac|client|...]

```

end

## config system global

Parameter	Description	Type	Size	Default						
admin-concurrent	Enable/disable concurrent administrator logins. Use policy-auth-concurrent for firewall authenticated users.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable admin concurrent login.</td></tr><tr><td><i>disable</i></td><td>Disable admin concurrent login.</td></tr></table>	Option	Description	<i>enable</i>	Enable admin concurrent login.	<i>disable</i>	Disable admin concurrent login.			
Option	Description									
<i>enable</i>	Enable admin concurrent login.									
<i>disable</i>	Disable admin concurrent login.									

Parameter	Description	Type	Size	Default						
admin-console-timeout	Console login timeout that overrides the admin timeout value.	integer	Minimum value: 15 Maximum value: 300	0						
admin-forticloud-sso-login	Enable/disable FortiCloud admin login via SSO.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable FortiCloud admin login via SSO.</td></tr><tr><td><i>disable</i></td><td>Disable FortiCloud admin login via SSO.</td></tr></table>	Option	Description	<i>enable</i>	Enable FortiCloud admin login via SSO.	<i>disable</i>	Disable FortiCloud admin login via SSO.			
Option	Description									
<i>enable</i>	Enable FortiCloud admin login via SSO.									
<i>disable</i>	Disable FortiCloud admin login via SSO.									
admin-host	Administrative host for HTTP and HTTPS. When set, will be used in lieu of the client's Host header for any redirection.	string	Maximum length: 255							
admin-hsts-max-age	HTTPS Strict-Transport-Security header max-age in seconds. A value of 0 will reset any HSTS records in the browser. When admin-https-redirect is disabled the header max-age will be 0.	integer	Minimum value: 0 Maximum value: 2147483647	15552000						
admin-https-pki-required	Enable/disable admin login method. Enable to force administrators to provide a valid certificate to log in if PKI is enabled. Disable to allow administrators to log in with a certificate or password.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Admin users must provide a valid certificate when PKI is enabled for HTTPS admin access.</td></tr><tr><td><i>disable</i></td><td>Admin users can login by providing a valid certificate or password.</td></tr></table>	Option	Description	<i>enable</i>	Admin users must provide a valid certificate when PKI is enabled for HTTPS admin access.	<i>disable</i>	Admin users can login by providing a valid certificate or password.			
Option	Description									
<i>enable</i>	Admin users must provide a valid certificate when PKI is enabled for HTTPS admin access.									
<i>disable</i>	Admin users can login by providing a valid certificate or password.									

Parameter	Description	Type	Size	Default																																		
admin-https-redirect	Enable/disable redirection of HTTP administration access to HTTPS.	option	-	enable																																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable redirecting HTTP administration access to HTTPS.</td></tr><tr><td><i>disable</i></td><td>Disable redirecting HTTP administration access to HTTPS.</td></tr></table>	Option	Description	<i>enable</i>	Enable redirecting HTTP administration access to HTTPS.	<i>disable</i>	Disable redirecting HTTP administration access to HTTPS.																															
Option	Description																																					
<i>enable</i>	Enable redirecting HTTP administration access to HTTPS.																																					
<i>disable</i>	Disable redirecting HTTP administration access to HTTPS.																																					
admin-https-ssl-banned-ciphers	Select one or more cipher technologies that cannot be used in GUI HTTPS negotiations. Only applies to TLS 1.2 and below.	option	-																																			
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>RSA</i></td><td>Ban the use of cipher suites using RSA key.</td></tr><tr><td><i>DHE</i></td><td>Ban the use of cipher suites using authenticated ephemeral DH key agreement.</td></tr><tr><td><i>ECDHE</i></td><td>Ban the use of cipher suites using authenticated ephemeral ECDH key agreement.</td></tr><tr><td><i>DSS</i></td><td>Ban the use of cipher suites using DSS authentication.</td></tr><tr><td><i>ECDSA</i></td><td>Ban the use of cipher suites using ECDSA authentication.</td></tr><tr><td><i>AES</i></td><td>Ban the use of cipher suites using either 128 or 256 bit AES.</td></tr><tr><td><i>AESGCM</i></td><td>Ban the use of cipher suites using AES in Galois Counter Mode (GCM).</td></tr><tr><td><i>CAMELLIA</i></td><td>Ban the use of cipher suites using either 128 or 256 bit CAMELLIA.</td></tr><tr><td><i>3DES</i></td><td>Ban the use of cipher suites using triple DES.</td></tr><tr><td><i>SHA1</i></td><td>Ban the use of cipher suites using HMAC-SHA1.</td></tr><tr><td><i>SHA256</i></td><td>Ban the use of cipher suites using HMAC-SHA256.</td></tr><tr><td><i>SHA384</i></td><td>Ban the use of cipher suites using HMAC-SHA384.</td></tr><tr><td><i>STATIC</i></td><td>Ban the use of cipher suites using static keys.</td></tr><tr><td><i>CHACHA20</i></td><td>Ban the use of cipher suites using ChaCha20.</td></tr><tr><td><i>ARIA</i></td><td>Ban the use of cipher suites using ARIA.</td></tr><tr><td><i>AESCCM</i></td><td>Ban the use of cipher suites using AESCCM.</td></tr></table>	Option	Description	<i>RSA</i>	Ban the use of cipher suites using RSA key.	<i>DHE</i>	Ban the use of cipher suites using authenticated ephemeral DH key agreement.	<i>ECDHE</i>	Ban the use of cipher suites using authenticated ephemeral ECDH key agreement.	<i>DSS</i>	Ban the use of cipher suites using DSS authentication.	<i>ECDSA</i>	Ban the use of cipher suites using ECDSA authentication.	<i>AES</i>	Ban the use of cipher suites using either 128 or 256 bit AES.	<i>AESGCM</i>	Ban the use of cipher suites using AES in Galois Counter Mode (GCM).	<i>CAMELLIA</i>	Ban the use of cipher suites using either 128 or 256 bit CAMELLIA.	<i>3DES</i>	Ban the use of cipher suites using triple DES.	<i>SHA1</i>	Ban the use of cipher suites using HMAC-SHA1.	<i>SHA256</i>	Ban the use of cipher suites using HMAC-SHA256.	<i>SHA384</i>	Ban the use of cipher suites using HMAC-SHA384.	<i>STATIC</i>	Ban the use of cipher suites using static keys.	<i>CHACHA20</i>	Ban the use of cipher suites using ChaCha20.	<i>ARIA</i>	Ban the use of cipher suites using ARIA.	<i>AESCCM</i>	Ban the use of cipher suites using AESCCM.			
Option	Description																																					
<i>RSA</i>	Ban the use of cipher suites using RSA key.																																					
<i>DHE</i>	Ban the use of cipher suites using authenticated ephemeral DH key agreement.																																					
<i>ECDHE</i>	Ban the use of cipher suites using authenticated ephemeral ECDH key agreement.																																					
<i>DSS</i>	Ban the use of cipher suites using DSS authentication.																																					
<i>ECDSA</i>	Ban the use of cipher suites using ECDSA authentication.																																					
<i>AES</i>	Ban the use of cipher suites using either 128 or 256 bit AES.																																					
<i>AESGCM</i>	Ban the use of cipher suites using AES in Galois Counter Mode (GCM).																																					
<i>CAMELLIA</i>	Ban the use of cipher suites using either 128 or 256 bit CAMELLIA.																																					
<i>3DES</i>	Ban the use of cipher suites using triple DES.																																					
<i>SHA1</i>	Ban the use of cipher suites using HMAC-SHA1.																																					
<i>SHA256</i>	Ban the use of cipher suites using HMAC-SHA256.																																					
<i>SHA384</i>	Ban the use of cipher suites using HMAC-SHA384.																																					
<i>STATIC</i>	Ban the use of cipher suites using static keys.																																					
<i>CHACHA20</i>	Ban the use of cipher suites using ChaCha20.																																					
<i>ARIA</i>	Ban the use of cipher suites using ARIA.																																					
<i>AESCCM</i>	Ban the use of cipher suites using AESCCM.																																					



Parameter	Description	Type	Size	Default
admin-https-ssl-ciphersuites	Select one or more TLS 1.3 ciphersuites to enable. Does not affect ciphers in TLS 1.2 and below. At least one must be enabled. To disable all, remove TLS1.3 from admin-https-ssl-versions.	option	-	TLS-AES-128-GCM-SHA256 TLS-AES-256-GCM-SHA384 TLS-CHACHA20-POLY1305-SHA256
	<b>Option</b>	<b>Description</b>		
	TLS-AES-128-GCM-SHA256	Enable TLS-AES-128-GCM-SHA256 in TLS 1.3.		
	TLS-AES-256-GCM-SHA384	Enable TLS-AES-256-GCM-SHA384 in TLS 1.3.		
	TLS-CHACHA20-POLY1305-SHA256	Enable TLS-CHACHA20-POLY1305-SHA256 in TLS 1.3.		
	TLS-AES-128-CCM-SHA256	Enable TLS-AES-128-CCM-SHA256 in TLS 1.3.		
	TLS-AES-128-CCM-8-SHA256	Enable TLS-AES-128-CCM-8-SHA256 in TLS 1.3.		
admin-https-ssl-versions	Allowed TLS versions for web administration.	option	-	tlsv1-2 tlsv1-3
	<b>Option</b>	<b>Description</b>		
	tlsv1-1	TLS 1.1.		
	tlsv1-2	TLS 1.2.		
	tlsv1-3	TLS 1.3.		
admin-lockout-duration	Amount of time in seconds that an administrator account is locked out after reaching the admin-lockout-threshold for repeated failed login attempts.	integer	Minimum value: 60 1 Maximum value: 2147483647	

Parameter	Description	Type	Size	Default						
admin-lockout-threshold	Number of failed login attempts before an administrator account is locked out for the admin-lockout-duration.	integer	Minimum value: 1 Maximum value: 10	3						
admin-login-max	Maximum number of administrators who can be logged in at the same time.	integer	Minimum value: 1 Maximum value: 100	100						
admin-maintainer	Enable/disable maintainer administrator login. When enabled, the maintainer account can be used to log in from the console after a hard reboot. The password is "bcpb" followed by the FortiGate unit serial number. You have limited time to complete this login.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable login for special user (maintainer).</td></tr><tr><td>disable</td><td>Disable login for special user (maintainer).</td></tr></table>				Option	Description	enable	Enable login for special user (maintainer).	disable	Disable login for special user (maintainer).
Option	Description									
enable	Enable login for special user (maintainer).									
disable	Disable login for special user (maintainer).									
admin-port	Administrative access port for HTTP..	integer	Minimum value: 80 Maximum value: 65535							
admin-reset-button *	press the reset button can reset to factory default	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>press the reset button can reset to factory default</td></tr><tr><td>disable</td><td>press the reset button cannot reset to factory default</td></tr></table>				Option	Description	enable	press the reset button can reset to factory default	disable	press the reset button cannot reset to factory default
Option	Description									
enable	press the reset button can reset to factory default									
disable	press the reset button cannot reset to factory default									
admin-restrict-local	Enable/disable local admin authentication restriction when remote authenticator is up and running.	option	-	disable						

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable local admin authentication restriction.		
	<i>disable</i>	Disable local admin authentication restriction.		
admin-scp	Enable/disable using SCP to download the system configuration. You can use SCP as an alternative method for backing up the configuration.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable allow system configuration download by SCP.		
	<i>disable</i>	Disable allow system configuration download by SCP.		
admin-server-cert	Server certificate that the FortiGate uses for HTTPS administrative connections.	string	Maximum length: 35	self-sign
admin-sport	Administrative access port for HTTPS..	integer	Minimum value: 1 Maximum value: 65535	443
admin-ssh-grace-time	Maximum time in seconds permitted between making an SSH connection to the FortiGate unit and authenticating.	integer	Minimum value: 10 Maximum value: 3600	120
admin-ssh-password	Enable/disable password authentication for SSH admin access.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable password authentication for SSH admin access.		
	<i>disable</i>	Disable password authentication for SSH admin access.		
admin-ssh-port	Administrative access port for SSH..	integer	Minimum value: 1 Maximum value: 65535	22

Parameter	Description	Type	Size	Default						
admin-ssh-v1	Enable/disable SSH v1 compatibility.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable SSH v1 compatibility.</td></tr><tr><td><i>disable</i></td><td>Disable SSH v1 compatibility.</td></tr></table>	Option	Description	<i>enable</i>	Enable SSH v1 compatibility.	<i>disable</i>	Disable SSH v1 compatibility.			
Option	Description									
<i>enable</i>	Enable SSH v1 compatibility.									
<i>disable</i>	Disable SSH v1 compatibility.									
admin-telnet	Enable/disable TELNET service.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable TELNET service.</td></tr><tr><td><i>disable</i></td><td>Disable TELNET service.</td></tr></table>	Option	Description	<i>enable</i>	Enable TELNET service.	<i>disable</i>	Disable TELNET service.			
Option	Description									
<i>enable</i>	Enable TELNET service.									
<i>disable</i>	Disable TELNET service.									
admin-telnet-port	Administrative access port for TELNET..	integer	Minimum value: 1 Maximum value: 65535	23						
admintimeout	Number of minutes before an idle administrator session times out. A shorter idle timeout is more secure.	integer	Minimum value: 1 Maximum value: 480	5						
alias	Alias for your FortiGate unit.	string	Maximum length: 35							
allow-traffic-redirect	Disable to prevent traffic with same local ingress and egress interface from being forwarded without policy check.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable allow traffic redirect.</td></tr><tr><td><i>disable</i></td><td>Disable allow traffic redirect.</td></tr></table>	Option	Description	<i>enable</i>	Enable allow traffic redirect.	<i>disable</i>	Disable allow traffic redirect.			
Option	Description									
<i>enable</i>	Enable allow traffic redirect.									
<i>disable</i>	Disable allow traffic redirect.									
anti-replay	Level of checking for packet replay and TCP sequence checking.	option	-	strict						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable anti-replay check.</td></tr></table>	Option	Description	<i>disable</i>	Disable anti-replay check.					
Option	Description									
<i>disable</i>	Disable anti-replay check.									

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>loose</i></td><td>Loose anti-replay check.</td></tr><tr><td><i>strict</i></td><td>Strict anti-replay check.</td></tr></table>				Option	Description	<i>loose</i>	Loose anti-replay check.	<i>strict</i>	Strict anti-replay check.
	Option	Description								
	<i>loose</i>	Loose anti-replay check.								
<i>strict</i>	Strict anti-replay check.									
arp-max-entry	Maximum number of dynamically learned MAC addresses that can be added to the ARP table.	integer	Minimum value: 131072 Maximum value: 2147483647	131072						
auth-cert	Server certificate that the FortiGate uses for HTTPS firewall authentication connections.	string	Maximum length: 35	Fortinet_Factory						
auth-http-port	User authentication HTTP port..	integer	Minimum value: 1 Maximum value: 65535	1000						
auth-https-port	User authentication HTTPS port..	integer	Minimum value: 1 Maximum value: 65535	1003						
auth-keepalive	Enable to prevent user authentication sessions from timing out when idle.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable use of keep alive to extend authentication.</td></tr><tr><td><i>disable</i></td><td>Disable use of keep alive to extend authentication.</td></tr></table>				Option	Description	<i>enable</i>	Enable use of keep alive to extend authentication.	<i>disable</i>	Disable use of keep alive to extend authentication.
	Option	Description								
	<i>enable</i>	Enable use of keep alive to extend authentication.								
<i>disable</i>	Disable use of keep alive to extend authentication.									
auth-session-limit	Action to take when the number of allowed user authenticated sessions is reached.	option	-	block-new						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>block-new</i></td><td>Block new user authentication attempts.</td></tr><tr><td><i>logout-inactive</i></td><td>Logout the most inactive user authenticated sessions.</td></tr></table>				Option	Description	<i>block-new</i>	Block new user authentication attempts.	<i>logout-inactive</i>	Logout the most inactive user authenticated sessions.
	Option	Description								
	<i>block-new</i>	Block new user authentication attempts.								
<i>logout-inactive</i>	Logout the most inactive user authenticated sessions.									

Parameter	Description	Type	Size	Default								
auto-auth-extension-device	Enable/disable automatic authorization of dedicated Fortinet extension devices.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable automatic authorization of dedicated Fortinet extension device globally.</td></tr><tr><td><i>disable</i></td><td>Disable automatic authorization of dedicated Fortinet extension device globally.</td></tr></table>	Option	Description	<i>enable</i>	Enable automatic authorization of dedicated Fortinet extension device globally.	<i>disable</i>	Disable automatic authorization of dedicated Fortinet extension device globally.					
Option	Description											
<i>enable</i>	Enable automatic authorization of dedicated Fortinet extension device globally.											
<i>disable</i>	Disable automatic authorization of dedicated Fortinet extension device globally.											
autorun-log-fsck	Enable/disable automatic log partition check after ungraceful shutdown.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable automatic log partition check after ungraceful shutdown.</td></tr><tr><td><i>disable</i></td><td>Disable automatic log partition check after ungraceful shutdown.</td></tr></table>	Option	Description	<i>enable</i>	Enable automatic log partition check after ungraceful shutdown.	<i>disable</i>	Disable automatic log partition check after ungraceful shutdown.					
Option	Description											
<i>enable</i>	Enable automatic log partition check after ungraceful shutdown.											
<i>disable</i>	Disable automatic log partition check after ungraceful shutdown.											
av-affinity *	Affinity setting for AV scanning (hexadecimal value up to 256 bits in the format of xxxxxxxxxxxxxxxx).	string	Maximum length: 79	0								
av-failopen	Set the action to take if the FortiGate is running low on memory or the proxy connection limit has been reached.	option	-	pass								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>pass</i></td><td>Bypass the antivirus system when memory is low. Antivirus scanning resumes when the low memory condition is resolved.</td></tr><tr><td><i>off</i></td><td>Stop accepting new AV sessions when entering conserve mode, but continue to process current active sessions.</td></tr><tr><td><i>one-shot</i></td><td>Bypass the antivirus system when memory is low.</td></tr></table>	Option	Description	<i>pass</i>	Bypass the antivirus system when memory is low. Antivirus scanning resumes when the low memory condition is resolved.	<i>off</i>	Stop accepting new AV sessions when entering conserve mode, but continue to process current active sessions.	<i>one-shot</i>	Bypass the antivirus system when memory is low.			
Option	Description											
<i>pass</i>	Bypass the antivirus system when memory is low. Antivirus scanning resumes when the low memory condition is resolved.											
<i>off</i>	Stop accepting new AV sessions when entering conserve mode, but continue to process current active sessions.											
<i>one-shot</i>	Bypass the antivirus system when memory is low.											

Parameter	Description	Type	Size	Default						
av-failopen-session	When enabled and a proxy for a protocol runs out of room in its session table, that protocol goes into failopen mode and enacts the action specified by av-failopen.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable AV fail open session option.</td></tr><tr><td><i>disable</i></td><td>Disable AV fail open session option.</td></tr></table>	Option	Description	<i>enable</i>	Enable AV fail open session option.	<i>disable</i>	Disable AV fail open session option.			
	Option	Description								
	<i>enable</i>	Enable AV fail open session option.								
<i>disable</i>	Disable AV fail open session option.									
batch-cmdb	Enable/disable batch mode, allowing you to enter a series of CLI commands that will execute as a group once they are loaded.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable batch mode to execute in CMDB server.</td></tr><tr><td><i>disable</i></td><td>Disable batch mode to execute in CMDB server.</td></tr></table>	Option	Description	<i>enable</i>	Enable batch mode to execute in CMDB server.	<i>disable</i>	Disable batch mode to execute in CMDB server.			
	Option	Description								
	<i>enable</i>	Enable batch mode to execute in CMDB server.								
<i>disable</i>	Disable batch mode to execute in CMDB server.									
block-session-timer	Duration in seconds for blocked sessions.	integer	Minimum value: 30 1 Maximum value: 300							
br-fdb-max-entry	Maximum number of bridge forwarding database (FDB) entries.	integer	Minimum value: 8192 Maximum value: 2147483647							
cert-chain-max	Maximum number of certificates that can be traversed in a certificate chain.	integer	Minimum value: 8 1 Maximum value: 2147483647							
cfg-revert-timeout	Time-out for reverting to the last saved configuration..	integer	Minimum value: 600 10 Maximum value: 4294967295							
cfg-save	Configuration file save mode for CLI changes.	option	-	automatic						

Parameter	Description	Type	Size	Default
	<b>Option</b> <b>Description</b>			
	<i>automatic</i>	Automatically save config.		
	<i>manual</i>	Manually save config.		
	<i>revert</i>	Manually save config and revert the config when timeout.		
check-protocol-header	Level of checking performed on protocol headers. Strict checking is more thorough but may affect performance. Loose checking is OK in most cases.	option	-	loose
	<b>Option</b> <b>Description</b>			
	<i>loose</i>	Check protocol header loosely.		
	<i>strict</i>	Check protocol header strictly.		
check-reset-range	Configure ICMP error message verification. You can either apply strict RST range checking or disable it.	option	-	disable
	<b>Option</b> <b>Description</b>			
	<i>strict</i>	Check RST range strictly.		
	<i>disable</i>	Disable RST range check.		
cli-audit-log	Enable/disable CLI audit log.	option	-	disable
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Enable CLI audit log.		
	<i>disable</i>	Disable CLI audit log.		
cloud-communication	Enable/disable all cloud communication.	option	-	enable
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Allow cloud communication.		
	<i>disable</i>	Disable all cloud-related settings.		



Parameter	Description	Type	Size	Default
clt-cert-req	Enable/disable requiring administrators to have a client certificate to log into the GUI using HTTPS.	option	-	disable
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Enable require client certificate for GUI login.		
	<i>disable</i>	Disable require client certificate for GUI login.		
cmdbsvr-affinity	Affinity setting for cmdbsvr (hexadecimal value up to 256 bits in the format of xxxxxxxxxxxxxxxx).	string	Maximum length: 79	0
cpu-use-threshold	Threshold at which CPU usage is reported.	integer	Minimum value: 50 Maximum value: 99	90
csr-ca-attribute	Enable/disable the CA attribute in certificates. Some CA servers reject CSRs that have the CA attribute.	option	-	enable
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Enable CA attribute in CSR.		
	<i>disable</i>	Disable CA attribute in CSR.		
daily-restart	Enable/disable daily restart of FortiGate unit. Use the restart-time option to set the time of day for the restart.	option	-	disable
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Enable daily reboot of the FortiGate.		
	<i>disable</i>	Disable daily reboot of the FortiGate.		
default-service-source-port	Default service source port range.	user	Not Specified	

Parameter	Description	Type	Size	Default																
device-idle-timeout	Time in seconds that a device must be idle to automatically log the device user out..	integer	Minimum value: 30 Maximum value: 31536000	300																
dh-params	Number of bits to use in the Diffie-Hellman exchange for HTTPS/SSH protocols.	option	-	2048																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>1024</td><td>1024 bits.</td></tr><tr><td>1536</td><td>1536 bits.</td></tr><tr><td>2048</td><td>2048 bits.</td></tr><tr><td>3072</td><td>3072 bits.</td></tr><tr><td>4096</td><td>4096 bits.</td></tr><tr><td>6144</td><td>6144 bits.</td></tr><tr><td>8192</td><td>8192 bits.</td></tr></table>				Option	Description	1024	1024 bits.	1536	1536 bits.	2048	2048 bits.	3072	3072 bits.	4096	4096 bits.	6144	6144 bits.	8192	8192 bits.
	Option	Description																		
	1024	1024 bits.																		
	1536	1536 bits.																		
	2048	2048 bits.																		
	3072	3072 bits.																		
	4096	4096 bits.																		
	6144	6144 bits.																		
8192	8192 bits.																			
dnsproxy-worker-count	DNS proxy worker count. For a FortiGate with multiple logical CPUs, you can set the DNS process number from 1 to the number of logical CPUs.	integer	Minimum value: 1 Maximum value: 8 **	1																
dst	Enable/disable daylight saving time.	option	-	enable																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable daylight saving time.</td></tr><tr><td>disable</td><td>Disable daylight saving time.</td></tr></table>				Option	Description	enable	Enable daylight saving time.	disable	Disable daylight saving time.										
	Option	Description																		
	enable	Enable daylight saving time.																		
disable	Disable daylight saving time.																			
early-tcp-npu-session	Enable/disable early TCP NPU session.	option	-	disable																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable early TCP NPU session in order to guarantee packet order of 3-way handshake.</td></tr><tr><td>disable</td><td>Disable early TCP NPU session in order to guarantee packet order of 3-way handshake.</td></tr></table>				Option	Description	enable	Enable early TCP NPU session in order to guarantee packet order of 3-way handshake.	disable	Disable early TCP NPU session in order to guarantee packet order of 3-way handshake.										
	Option	Description																		
	enable	Enable early TCP NPU session in order to guarantee packet order of 3-way handshake.																		
disable	Disable early TCP NPU session in order to guarantee packet order of 3-way handshake.																			

Parameter	Description	Type	Size	Default						
edit-vdom-prompt *	Enable/disable edit new VDOM prompt.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable edit new VDOM prompt.</td></tr><tr><td><i>disable</i></td><td>Disable edit new VDOM prompt.</td></tr></table>	Option	Description	<i>enable</i>	Enable edit new VDOM prompt.	<i>disable</i>	Disable edit new VDOM prompt.			
Option	Description									
<i>enable</i>	Enable edit new VDOM prompt.									
<i>disable</i>	Disable edit new VDOM prompt.									
extender-controller-reserved-network	Configure reserved network subnet for managed LAN extension FortiExtender units. This is available when the FortiExtender daemon is running.	ipv4-classnet-host	Not Specified	10.252.0.1 255.255.0.0						
failtime	Fail-time for server lost.	integer	Minimum value: 0 Maximum value: 4294967295	5						
faz-disk-buffer-size	Maximum disk buffer size to temporarily store logs destined for FortiAnalyzer. To be used in the event that FortiAnalyzer is unavailable.	integer	Minimum value: 0 Maximum value: 214748364	0						
fds-statistics	Enable/disable sending IPS, Application Control, and AntiVirus data to FortiGuard. This data is used to improve FortiGuard services and is not shared with external parties and is protected by Fortinet's privacy policy.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable FortiGuard statistics.</td></tr><tr><td><i>disable</i></td><td>Disable FortiGuard statistics.</td></tr></table>	Option	Description	<i>enable</i>	Enable FortiGuard statistics.	<i>disable</i>	Disable FortiGuard statistics.			
Option	Description									
<i>enable</i>	Enable FortiGuard statistics.									
<i>disable</i>	Disable FortiGuard statistics.									
fds-statistics-period	FortiGuard statistics collection period in minutes..	integer	Minimum value: 1 Maximum value: 1440	60						

Parameter	Description	Type	Size	Default														
fgd-alert-subscription	Type of alert to retrieve from FortiGuard.	option	-															
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>advisory</i></td><td>Retrieve FortiGuard advisories, report and news alerts.</td></tr><tr><td><i>latest-threat</i></td><td>Retrieve latest FortiGuard threats alerts.</td></tr><tr><td><i>latest-virus</i></td><td>Retrieve latest FortiGuard virus alerts.</td></tr><tr><td><i>latest-attack</i></td><td>Retrieve latest FortiGuard attack alerts.</td></tr><tr><td><i>new-antivirus-db</i></td><td>Retrieve FortiGuard AV database release alerts.</td></tr><tr><td><i>new-attack-db</i></td><td>Retrieve FortiGuard IPS database release alerts.</td></tr></table>	Option	Description	<i>advisory</i>	Retrieve FortiGuard advisories, report and news alerts.	<i>latest-threat</i>	Retrieve latest FortiGuard threats alerts.	<i>latest-virus</i>	Retrieve latest FortiGuard virus alerts.	<i>latest-attack</i>	Retrieve latest FortiGuard attack alerts.	<i>new-antivirus-db</i>	Retrieve FortiGuard AV database release alerts.	<i>new-attack-db</i>	Retrieve FortiGuard IPS database release alerts.			
Option	Description																	
<i>advisory</i>	Retrieve FortiGuard advisories, report and news alerts.																	
<i>latest-threat</i>	Retrieve latest FortiGuard threats alerts.																	
<i>latest-virus</i>	Retrieve latest FortiGuard virus alerts.																	
<i>latest-attack</i>	Retrieve latest FortiGuard attack alerts.																	
<i>new-antivirus-db</i>	Retrieve FortiGuard AV database release alerts.																	
<i>new-attack-db</i>	Retrieve FortiGuard IPS database release alerts.																	
forticarrier-bypass *	Enable/disable forticarrier-bypass.	option	-	disable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable FortiCarrier bypass.</td></tr><tr><td><i>disable</i></td><td>Disable FortiCarrier bypass.</td></tr></table>	Option	Description	<i>enable</i>	Enable FortiCarrier bypass.	<i>disable</i>	Disable FortiCarrier bypass.											
Option	Description																	
<i>enable</i>	Enable FortiCarrier bypass.																	
<i>disable</i>	Disable FortiCarrier bypass.																	
forticontroller-proxy *	Enable/disable FortiController proxy.	option	-	enable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.											
Option	Description																	
<i>enable</i>	Enable setting.																	
<i>disable</i>	Disable setting.																	
forticontroller-proxy-port *	FortiController proxy port.	integer	Minimum value: 1024 Maximum value: 49150	11133														
fortiextender	Enable/disable FortiExtender.	option	-	disable **														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable FortiExtender controller.</td></tr><tr><td><i>enable</i></td><td>Enable FortiExtender controller.</td></tr></table>	Option	Description	<i>disable</i>	Disable FortiExtender controller.	<i>enable</i>	Enable FortiExtender controller.											
Option	Description																	
<i>disable</i>	Disable FortiExtender controller.																	
<i>enable</i>	Enable FortiExtender controller.																	
fortiextender-data-port	FortiExtender data port.	integer	Minimum value: 1024 Maximum value: 49150	25246														

Parameter	Description	Type	Size	Default
fortiextender-discovery-lockdown	Enable/disable FortiExtender CAPWAP lockdown.	option	-	disable
fortiextender-vlan-mode	Enable/disable FortiExtender VLAN mode.	option	-	disable
fortiservice-port	FortiService port. Used by FortiClient endpoint compliance. Older versions of FortiClient used a different port.	integer	Minimum value: 1 Maximum value: 65535	8013
fortitoken-cloud	Enable/disable FortiToken Cloud service.	option	-	enable
gui-allow-default-hostname	Enable/disable the factory default hostname warning on the GUI setup wizard.	option	-	disable

Parameter	Description	Type	Size	Default						
gui-allow-incompatible-fabric-fgt	Enable/disable Allow FGT with incompatible firmware to be treated as compatible in security fabric on the GUI. May cause unexpected error.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Display the feature in GUI.</td></tr><tr><td><i>disable</i></td><td>Do not display the feature in GUI.</td></tr></table>	Option	Description	<i>enable</i>	Display the feature in GUI.	<i>disable</i>	Do not display the feature in GUI.			
Option	Description									
<i>enable</i>	Display the feature in GUI.									
<i>disable</i>	Do not display the feature in GUI.									
gui-cdn-domain-override	Domain of CDN server.	string	Maximum length: 255							
gui-cdn-usage	Enable/disable Load GUI static files from a CDN.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Display the feature in GUI.</td></tr><tr><td><i>disable</i></td><td>Do not display the feature in GUI.</td></tr></table>	Option	Description	<i>enable</i>	Display the feature in GUI.	<i>disable</i>	Do not display the feature in GUI.			
Option	Description									
<i>enable</i>	Display the feature in GUI.									
<i>disable</i>	Do not display the feature in GUI.									
gui-certificates	Enable/disable the System > Certificate GUI page, allowing you to add and configure certificates from the GUI.	option	-	enable **						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Display the feature in GUI.</td></tr><tr><td><i>disable</i></td><td>Do not display the feature in GUI.</td></tr></table>	Option	Description	<i>enable</i>	Display the feature in GUI.	<i>disable</i>	Do not display the feature in GUI.			
Option	Description									
<i>enable</i>	Display the feature in GUI.									
<i>disable</i>	Do not display the feature in GUI.									
gui-custom-language	Enable/disable custom languages in GUI.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Display the feature in GUI.</td></tr><tr><td><i>disable</i></td><td>Do not display the feature in GUI.</td></tr></table>	Option	Description	<i>enable</i>	Display the feature in GUI.	<i>disable</i>	Do not display the feature in GUI.			
Option	Description									
<i>enable</i>	Display the feature in GUI.									
<i>disable</i>	Do not display the feature in GUI.									
gui-date-format	Default date format used throughout GUI.	option	-	yyyy/MM/dd						

Parameter	Description	Type	Size	Default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>yyyy/MM/dd</i></td><td>Year/Month/Day.</td></tr><tr><td><i>dd/MM/yyyy</i></td><td>Day/Month/Year.</td></tr><tr><td><i>MM/dd/yyyy</i></td><td>Month/Day/Year.</td></tr><tr><td><i>yyyy-MM-dd</i></td><td>Year-Month-Day.</td></tr><tr><td><i>dd-MM-yyyy</i></td><td>Day-Month-Year.</td></tr><tr><td><i>MM-dd-yyyy</i></td><td>Month-Day-Year.</td></tr></table>	Option	Description	<i>yyyy/MM/dd</i>	Year/Month/Day.	<i>dd/MM/yyyy</i>	Day/Month/Year.	<i>MM/dd/yyyy</i>	Month/Day/Year.	<i>yyyy-MM-dd</i>	Year-Month-Day.	<i>dd-MM-yyyy</i>	Day-Month-Year.	<i>MM-dd-yyyy</i>	Month-Day-Year.			
	Option	Description																
	<i>yyyy/MM/dd</i>	Year/Month/Day.																
	<i>dd/MM/yyyy</i>	Day/Month/Year.																
	<i>MM/dd/yyyy</i>	Month/Day/Year.																
	<i>yyyy-MM-dd</i>	Year-Month-Day.																
	<i>dd-MM-yyyy</i>	Day-Month-Year.																
<i>MM-dd-yyyy</i>	Month-Day-Year.																	
gui-date-time-source	Source from which the FortiGate GUI uses to display date and time entries.	option	-	system														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>system</i></td><td>Use this FortiGate unit's configured timezone.</td></tr><tr><td><i>browser</i></td><td>Use the web browser's timezone.</td></tr></table>	Option	Description	<i>system</i>	Use this FortiGate unit's configured timezone.	<i>browser</i>	Use the web browser's timezone.											
	Option	Description																
	<i>system</i>	Use this FortiGate unit's configured timezone.																
<i>browser</i>	Use the web browser's timezone.																	
gui-device-latitude	Add the latitude of the location of this FortiGate to position it on the Threat Map.	string	Maximum length: 19															
gui-device-longitude	Add the longitude of the location of this FortiGate to position it on the Threat Map.	string	Maximum length: 19															
gui-display-hostname	Enable/disable displaying the FortiGate's hostname on the GUI login page.	option	-	disable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Display the feature in GUI.</td></tr><tr><td><i>disable</i></td><td>Do not display the feature in GUI.</td></tr></table>	Option	Description	<i>enable</i>	Display the feature in GUI.	<i>disable</i>	Do not display the feature in GUI.											
	Option	Description																
	<i>enable</i>	Display the feature in GUI.																
<i>disable</i>	Do not display the feature in GUI.																	
gui-firmware-upgrade-warning	Enable/disable the firmware upgrade warning on the GUI.	option	-	enable														

Parameter	Description	Type	Size	Default
	<b>Option</b>		<b>Description</b>	
	<i>enable</i>		Display the feature in GUI.	
	<i>disable</i>		Do not display the feature in GUI.	
gui-forticare-registration-setup-warning	Enable/disable the FortiCare registration setup warning on the GUI.	option	-	enable
	<b>Option</b>		<b>Description</b>	
	<i>enable</i>		Display the feature in GUI.	
	<i>disable</i>		Do not display the feature in GUI.	
gui-fortigate-cloud-sandbox	Enable/disable displaying FortiGate Cloud Sandbox on the GUI.	option	-	disable
	<b>Option</b>		<b>Description</b>	
	<i>enable</i>		Display the feature in GUI.	
	<i>disable</i>		Do not display the feature in GUI.	
gui-fortiguard-resource-fetch	Enable/disable retrieving static GUI resources from FortiGuard. Disabling it will improve GUI load time for air-gapped environments.	option	-	enable
	<b>Option</b>		<b>Description</b>	
	<i>enable</i>		Enable retrieving static GUI resources from FortiGuard.	
	<i>disable</i>		Disable retrieving static GUI resources from FortiGuard.	
gui-ipv6	Enable/disable IPv6 settings on the GUI.	option	-	disable
	<b>Option</b>		<b>Description</b>	
	<i>enable</i>		Display the feature in GUI.	
	<i>disable</i>		Do not display the feature in GUI.	
gui-local-out	Enable/disable Local-out traffic on the GUI.	option	-	disable



Parameter	Description	Type	Size	Default
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Display the feature in GUI.		
	<i>disable</i>	Do not display the feature in GUI.		
gui-replacement-message-groups	Enable/disable replacement message groups on the GUI.	option	-	disable
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Display the feature in GUI.		
	<i>disable</i>	Do not display the feature in GUI.		
gui-rest-api-cache	Enable/disable REST API result caching on FortiGate.	option	-	enable **
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Enable REST API result caching on FortiGate.		
	<i>disable</i>	Disable REST API result caching on FortiGate.		
gui-theme	Color scheme for the administration GUI.	option	-	jade
	<b>Option</b> <b>Description</b>			
	<i>jade</i>	Jade theme.		
	<i>neutrino</i>	Neutrino theme.		
	<i>mariner</i>	Mariner theme.		
	<i>graphite</i>	Graphite theme.		
	<i>melongene</i>	Melongene theme.		
	<i>retro</i>	FortiOS v3 Retro theme.		
	<i>dark-matter</i>	Dark Matter theme.		
	<i>onyx</i>	Onyx theme.		
	<i>eclipse</i>	Eclipse theme.		
gui-wireless-opensecurity	Enable/disable wireless open security option on the GUI.	option	-	disable

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Display the feature in GUI.		
	<i>disable</i>	Do not display the feature in GUI.		
ha-affinity	Affinity setting for HA daemons (hexadecimal value up to 256 bits in the format of xxxxxxxxxxxxxxxx).	string	Maximum length: 79	0
honor-df	Enable/disable honoring of Don't-Fragment (DF) flag.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable honoring of Don't-Fragment flag.		
	<i>disable</i>	Disable honoring of Don't-Fragment flag.		
hostname	FortiGate unit's hostname. Most models will truncate names longer than 24 characters. Some models support hostnames up to 35 characters.	string	Maximum length: 35	
hyper-scale-vdom-num *	Number of VDOMs for hyper scale license.	integer	Minimum value: 1 Maximum value: 250	250
igmp-state-limit	Maximum number of IGMP memberships.	integer	Minimum value: 96 Maximum value: 128000	3200
internal-switch-speed *	Internal port speed.	option	-	
	<b>Option</b>	<b>Description</b>		
	<i>auto</i>	auto		
	<i>1000full</i>	1000M Full		
	<i>100full</i>	100M full.		
	<i>100half</i>	100M half.		

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>10full</i></td><td>10M full.</td></tr><tr><td><i>10half</i></td><td>10M half.</td></tr></table>	Option	Description	<i>10full</i>	10M full.	<i>10half</i>	10M half.					
	Option	Description										
	<i>10full</i>	10M full.										
	<i>10half</i>	10M half.										
internet-service-database	Configure which Internet Service database size to download from FortiGuard and use.	option	-	full **								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>mini</i></td><td>Small sized Internet Service database with very limited IP addresses.</td></tr><tr><td><i>standard</i></td><td>Medium sized Internet Service database with most IP addresses.</td></tr><tr><td><i>full</i></td><td>Full sized Internet Service database with all IP addresses.</td></tr></table>	Option	Description	<i>mini</i>	Small sized Internet Service database with very limited IP addresses.	<i>standard</i>	Medium sized Internet Service database with most IP addresses.	<i>full</i>	Full sized Internet Service database with all IP addresses.			
	Option	Description										
	<i>mini</i>	Small sized Internet Service database with very limited IP addresses.										
	<i>standard</i>	Medium sized Internet Service database with most IP addresses.										
<i>full</i>	Full sized Internet Service database with all IP addresses.											
interval	Dead gateway detection interval.	integer	Minimum value: 0 Maximum value: 4294967295	5								
ip-fragment-mem-thresholds	Maximum memory (MB) used to reassemble IPv4/IPv6 fragments.	integer	Minimum value: 32 Maximum value: 2047	32								
ip-src-port-range	IP source port range used for traffic originating from the FortiGate unit.	user	Not Specified	1024-25000								
ips-affinity *	Affinity setting for IPS (hexadecimal value up to 256 bits in the format of xxxxxxxxxxxxxxxx; allowed CPUs must be less than total number of IPS engine daemons).	string	Maximum length: 79	0								
ipsec-asic-offload *	Enable/disable ASIC offloading (hardware acceleration) for IPsec VPN traffic. Hardware acceleration can offload IPsec VPN sessions and accelerate encryption and decryption.	option	-	enable								

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable ASIC offload for IPsec VPN.		
	<i>disable</i>	Disable ASIC offload for IPsec VPN.		
ipsec-ha-seqjump-rate	ESP jump ahead rate (1G - 10G pps equivalent).	integer	Minimum value: 10 1 Maximum value: 10	10
ipsec-hmac-offload *	Enable/disable offloading (hardware acceleration) of HMAC processing for IPsec VPN.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable offload IPsec HMAC processing to hardware if possible.		
	<i>disable</i>	Disable offload IPsec HMAC processing to hardware.		
ipsec-round-robin *	Enable/disable round-robin redistribution to multiple CPUs for IPsec VPN traffic.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable round-robin redistribution for IPsec VPN.		
	<i>disable</i>	Disable round-robin redistribution for IPsec VPN.		
ipsec-soft-dec-async	Enable/disable software decryption asynchronization (using multiple CPUs to do decryption) for IPsec VPN traffic.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable software decryption asynchronization for IPsec VPN.		
	<i>disable</i>	Disable software decryption asynchronization for IPsec VPN.		
ipv6-accept-dad	Enable/disable acceptance of IPv6 Duplicate Address Detection (DAD).	integer	Minimum value: 0 Maximum value: 2	1

Parameter	Description	Type	Size	Default
ipv6-allow-anycast-probe	Enable/disable IPv6 address probe through Anycast.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable probing of IPv6 address space through Anycast		
	<i>disable</i>	Disable probing of IPv6 address space through Anycast		
ipv6-allow-local-in-slient-drop	Enable/disable silent drop of IPv6 local-in traffic.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable silent drop of IPv6 local-in traffic.		
	<i>disable</i>	Disable silent drop of IPv6 local-in traffic.		
ipv6-allow-multicast-probe	Enable/disable IPv6 address probe through Multicast.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable probing of IPv6 address space through Multicast.		
	<i>disable</i>	Disable probing of IPv6 address space through Multicast.		
ipv6-allow-traffic-redirect	Disable to prevent IPv6 traffic with same local ingress and egress interface from being forwarded without policy check.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable allow traffic IPv6 redirect.		
	<i>disable</i>	Disable allow traffic IPv6 redirect.		
irq-time-accounting	Configure CPU IRQ time accounting mode.	option	-	auto
	<b>Option</b>	<b>Description</b>		
	<i>auto</i>	Automatically switch CPU accounting mode.		
	<i>force</i>	Force the use of CPU IRQ time accounting mode.		

Parameter	Description	Type	Size	Default
language	GUI display language.	option	-	english
	<b>Option</b>	<b>Description</b>		
	english	English.		
	french	French.		
	spanish	Spanish.		
	portuguese	Portuguese.		
	japanese	Japanese.		
	trach	Traditional Chinese.		
	simch	Simplified Chinese.		
	korean	Korean.		
ldapconntimeout	Global timeout for connections with remote LDAP servers in milliseconds.	integer	Minimum value: 1 Maximum value: 300000	500
legacy-poe-device-support *	Enable/disable legacy POE device support.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	enable	Enable legacy POE device support.		
	disable	Disable legacy POE device support.		
lldp-reception	Enable/disable Link Layer Discovery Protocol (LLDP) reception.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	enable	Enable reception of Link Layer Discovery Protocol (LLDP).		
	disable	Disable reception of Link Layer Discovery Protocol (LLDP).		
lldp-transmission	Enable/disable Link Layer Discovery Protocol (LLDP) transmission.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	enable	Enable transmission of Link Layer Discovery Protocol (LLDP).		
	disable	Disable transmission of Link Layer Discovery Protocol (LLDP).		

Parameter	Description	Type	Size	Default						
log-ssl-connection	Enable/disable logging of SSL connection events.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable logging of SSL connection events.</td></tr><tr><td><i>disable</i></td><td>Disable logging of SSL connection events.</td></tr></table>	Option	Description	<i>enable</i>	Enable logging of SSL connection events.	<i>disable</i>	Disable logging of SSL connection events.			
Option	Description									
<i>enable</i>	Enable logging of SSL connection events.									
<i>disable</i>	Disable logging of SSL connection events.									
log-uuid-address	Enable/disable insertion of address UUIDs to traffic logs.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable insertion of address UUID to traffic logs.</td></tr><tr><td><i>disable</i></td><td>Disable insertion of address UUID to traffic logs.</td></tr></table>	Option	Description	<i>enable</i>	Enable insertion of address UUID to traffic logs.	<i>disable</i>	Disable insertion of address UUID to traffic logs.			
Option	Description									
<i>enable</i>	Enable insertion of address UUID to traffic logs.									
<i>disable</i>	Disable insertion of address UUID to traffic logs.									
login-timestamp	Enable/disable login time recording.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable login time recording.</td></tr><tr><td><i>disable</i></td><td>Disable login time recording.</td></tr></table>	Option	Description	<i>enable</i>	Enable login time recording.	<i>disable</i>	Disable login time recording.			
Option	Description									
<i>enable</i>	Enable login time recording.									
<i>disable</i>	Disable login time recording.									
long-vdom-name *	Enable/disable long VDOM name support.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable long VDOM name support.</td></tr><tr><td><i>disable</i></td><td>Disable long VDOM name support.</td></tr></table>	Option	Description	<i>enable</i>	Enable long VDOM name support.	<i>disable</i>	Disable long VDOM name support.			
Option	Description									
<i>enable</i>	Enable long VDOM name support.									
<i>disable</i>	Disable long VDOM name support.									
management-ip	Management IP address of this FortiGate. Used to log into this FortiGate from another FortiGate in the Security Fabric.	string	Maximum length: 255							
management-port	Overriding port for management connection (Overrides admin port).	integer	Minimum value: 443 1 Maximum value: 65535							

Parameter	Description	Type	Size	Default
management-port-use-admin-sport	Enable/disable use of the admin-sport setting for the management port. If disabled, FortiGate will allow user to specify management-port.	option	-	enable
	Option	Description		
	enable	Enable use of the admin-sport setting for the management port.		
	disable	Disable use of the admin-sport setting for the management port.		
management-vdom	Management virtual domain name.	string	Maximum length: 31	root
max-route-cache-size	Maximum number of IP route cache entries.	integer	Minimum value: 0 Maximum value: 2147483647	0
memory-use-threshold-extreme	Threshold at which memory usage is considered extreme.	integer	Minimum value: 70 Maximum value: 97	95
memory-use-threshold-green	Threshold at which memory usage forces the FortiGate to exit conserve mode.	integer	Minimum value: 70 Maximum value: 97	82
memory-use-threshold-red	Threshold at which memory usage forces the FortiGate to enter conserve mode.	integer	Minimum value: 70 Maximum value: 97	88
miglog-affinity *	Affinity setting for logging (64-bit hexadecimal value in the format of xxxxxxxxxxxxxxxx).	string	Maximum length: 19	0
miglogd-children	Number of logging (miglogd) processes to be allowed to run. Higher number can reduce performance; lower number can slow log processing time. No logs will be dropped or lost if the number is changed.	integer	Minimum value: 0 Maximum value: 15	0



Parameter	Description	Type	Size	Default						
multi-factor-authentication	Enforce all login methods to require an additional authentication factor.	option	-	optional						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>optional</i></td><td>Do not enforce all login methods to require an additional authentication factor (controlled by user settings).</td></tr><tr><td><i>mandatory</i></td><td>Enforce all login methods to require an additional authentication factor.</td></tr></table>	Option	Description	<i>optional</i>	Do not enforce all login methods to require an additional authentication factor (controlled by user settings).	<i>mandatory</i>	Enforce all login methods to require an additional authentication factor.			
Option	Description									
<i>optional</i>	Do not enforce all login methods to require an additional authentication factor (controlled by user settings).									
<i>mandatory</i>	Enforce all login methods to require an additional authentication factor.									
ndp-max-entry	Maximum number of NDP table entries (set to 65,536 or higher; if set to 0, kernel holds 65,536 entries).	integer	Minimum value: 0 65536 Maximum value: 2147483647							
per-user-bal *	Enable/disable per-user block/allow list filter.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable per-user block/allow list filter.</td></tr><tr><td><i>disable</i></td><td>Disable per-user block/allow list filter.</td></tr></table>	Option	Description	<i>enable</i>	Enable per-user block/allow list filter.	<i>disable</i>	Disable per-user block/allow list filter.			
Option	Description									
<i>enable</i>	Enable per-user block/allow list filter.									
<i>disable</i>	Disable per-user block/allow list filter.									
pmtu-discovery	Enable/disable path MTU discovery.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable path MTU discovery.</td></tr><tr><td><i>disable</i></td><td>Disable path MTU discovery.</td></tr></table>	Option	Description	<i>enable</i>	Enable path MTU discovery.	<i>disable</i>	Disable path MTU discovery.			
Option	Description									
<i>enable</i>	Enable path MTU discovery.									
<i>disable</i>	Disable path MTU discovery.									
policy-auth-concurrent	Number of concurrent firewall use logins from the same user.	integer	Minimum value: 0 0 Maximum value: 100							
post-login-banner	Enable/disable displaying the administrator access disclaimer message after an administrator successfully logs in.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable post-login banner.</td></tr><tr><td><i>enable</i></td><td>Enable post-login banner.</td></tr></table>	Option	Description	<i>disable</i>	Disable post-login banner.	<i>enable</i>	Enable post-login banner.			
Option	Description									
<i>disable</i>	Disable post-login banner.									
<i>enable</i>	Enable post-login banner.									

Parameter	Description	Type	Size	Default						
pre-login-banner	Enable/disable displaying the administrator access disclaimer message on the login page before an administrator logs in.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable pre-login banner.</td></tr><tr><td><i>disable</i></td><td>Disable pre-login banner.</td></tr></table>	Option	Description	<i>enable</i>	Enable pre-login banner.	<i>disable</i>	Disable pre-login banner.			
Option	Description									
<i>enable</i>	Enable pre-login banner.									
<i>disable</i>	Disable pre-login banner.									
private-data-encryption	Enable/disable private data encryption using an AES 128-bit key or passphrase.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable private data encryption using an AES 128-bit key.</td></tr><tr><td><i>enable</i></td><td>Enable private data encryption using an AES 128-bit key.</td></tr></table>	Option	Description	<i>disable</i>	Disable private data encryption using an AES 128-bit key.	<i>enable</i>	Enable private data encryption using an AES 128-bit key.			
Option	Description									
<i>disable</i>	Disable private data encryption using an AES 128-bit key.									
<i>enable</i>	Enable private data encryption using an AES 128-bit key.									
proxy-auth-lifetime	Enable/disable authenticated users lifetime control. This is a cap on the total time a proxy user can be authenticated for after which re-authentication will take place.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable authenticated users lifetime control.</td></tr><tr><td><i>disable</i></td><td>Disable authenticated users lifetime control.</td></tr></table>	Option	Description	<i>enable</i>	Enable authenticated users lifetime control.	<i>disable</i>	Disable authenticated users lifetime control.			
Option	Description									
<i>enable</i>	Enable authenticated users lifetime control.									
<i>disable</i>	Disable authenticated users lifetime control.									
proxy-auth-lifetime-timeout	Lifetime timeout in minutes for authenticated users.	integer	Minimum value: 5 Maximum value: 65535	480						
proxy-auth-timeout	Authentication timeout in minutes for authenticated users.	integer	Minimum value: 1 Maximum value: 300	10						
proxy-cert-use-mgmt-vdom	Enable/disable using management VDOM to send requests.	option	-	disable						

Parameter	Description	Type	Size	Default
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
proxy-hardware-acceleration *	Enable/disable email proxy hardware acceleration.	option	-	enable
	<b>Option</b> <b>Description</b>			
	<i>disable</i>	Disable email proxy hardware acceleration.		
	<i>enable</i>	Enable email proxy hardware acceleration.		
proxy-re-authentication-mode	Control if users must re-authenticate after a session is closed, traffic has been idle, or from the point at which the user was first created.	option	-	session
	<b>Option</b> <b>Description</b>			
	<i>session</i>	Proxy re-authentication timeout begins at the closure of the session.		
	<i>traffic</i>	Proxy re-authentication timeout begins after traffic has not been received.		
	<i>absolute</i>	Proxy re-authentication timeout begins when the user was first created.		
proxy-resource-mode	Enable/disable use of the maximum memory usage on the FortiGate unit's proxy processing of resources, such as block lists, allow lists, and external resources.	option	-	disable
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Enable use of the maximum memory usage.		
	<i>disable</i>	Disable use of the maximum memory usage.		
proxy-worker-count	Proxy worker count.	integer	Minimum value: 1 Maximum value: 8 **	0

Parameter	Description	Type	Size	Default
radius-port	RADIUS service port number.	integer	Minimum value: 1 Maximum value: 65535	1812
reboot-upon-config-restore	Enable/disable reboot of system upon restoring configuration.	option	-	enable
	Option	Description		
	enable	Enable reboot of system upon restoring configuration.		
	disable	Disable reboot of system upon restoring configuration.		
refresh	Statistics refresh interval second(s) in GUI.	integer	Minimum value: 0 Maximum value: 4294967295	0
remoteauthtimeout	Number of seconds that the FortiGate waits for responses from remote RADIUS, LDAP, or TACACS+ authentication servers..	integer	Minimum value: 1 Maximum value: 300	5
reset-sessionless-tcp	Action to perform if the FortiGate receives a TCP packet but cannot find a corresponding session in its session table. NAT/Route mode only.	option	-	disable
	Option	Description		
	enable	Enable reset session-less TCP.		
	disable	Disable reset session-less TCP.		
restart-time	Daily restart time (hh:mm).	user	Not Specified	
revision-backup-on-logout	Enable/disable back-up of the latest configuration revision when an administrator logs out of the CLI or GUI.	option	-	disable

Parameter	Description	Type	Size	Default
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Enable revision config backup automatically when logout.		
	<i>disable</i>	Disable revision config backup automatically when logout.		
revision-image-auto-backup	Enable/disable back-up of the latest image revision after the firmware is upgraded.	option	-	disable
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Enable revision image backup automatically when upgrading image.		
	<i>disable</i>	Disable revision image backup automatically when upgrading image.		
scanunit-count	Number of scanunits. The range and the default depend on the number of CPUs. Only available on FortiGate units with multiple CPUs.	integer	Minimum value: 0 1 Maximum value: 8 **	
security-rating-result-submission	Enable/disable the submission of Security Rating results to FortiGuard.	option	-	enable
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Enable submission of Security Rating results to FortiGuard.		
	<i>disable</i>	Disable submission of Security Rating results to FortiGuard.		
security-rating-run-on-schedule	Enable/disable scheduled runs of Security Rating.	option	-	enable
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Enable scheduled runs of Security Rating.		
	<i>disable</i>	Disable scheduled runs of Security Rating.		

Parameter	Description	Type	Size	Default						
send-pmtu-icmp	Enable/disable sending of path maximum transmission unit (PMTU) - ICMP destination unreachable packet and to support PMTUD protocol on your network to reduce fragmentation of packets.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable sending of PMTU ICMP destination unreachable packet.</td></tr><tr><td><i>disable</i></td><td>Disable sending of PMTU ICMP destination unreachable packet.</td></tr></table>	Option	Description	<i>enable</i>	Enable sending of PMTU ICMP destination unreachable packet.	<i>disable</i>	Disable sending of PMTU ICMP destination unreachable packet.			
Option	Description									
<i>enable</i>	Enable sending of PMTU ICMP destination unreachable packet.									
<i>disable</i>	Disable sending of PMTU ICMP destination unreachable packet.									
show-backplane-intf *	show/hide backplane interfaces	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>show backplane interfaces</td></tr><tr><td><i>disable</i></td><td>hide backplane interfaces</td></tr></table>	Option	Description	<i>enable</i>	show backplane interfaces	<i>disable</i>	hide backplane interfaces			
Option	Description									
<i>enable</i>	show backplane interfaces									
<i>disable</i>	hide backplane interfaces									
snat-route-change	Enable/disable the ability to change the static NAT route.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable SNAT route change.</td></tr><tr><td><i>disable</i></td><td>Disable SNAT route change.</td></tr></table>	Option	Description	<i>enable</i>	Enable SNAT route change.	<i>disable</i>	Disable SNAT route change.			
Option	Description									
<i>enable</i>	Enable SNAT route change.									
<i>disable</i>	Disable SNAT route change.									
special-file-23-support	Enable/disable detection of those special format files when using Data Leak Protection.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable detection of those special format files when using Data Leak Protection.</td></tr><tr><td><i>enable</i></td><td>Enable detection of those special format files when using Data Leak Protection.</td></tr></table>	Option	Description	<i>disable</i>	Disable detection of those special format files when using Data Leak Protection.	<i>enable</i>	Enable detection of those special format files when using Data Leak Protection.			
Option	Description									
<i>disable</i>	Disable detection of those special format files when using Data Leak Protection.									
<i>enable</i>	Enable detection of those special format files when using Data Leak Protection.									
speedtest-server	Enable/disable speed test server.	option	-	disable						

Parameter	Description	Type	Size	Default												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable speed test server service.</td></tr><tr><td><i>disable</i></td><td>Disable speed test server service.</td></tr></table>	Option	Description	<i>enable</i>	Enable speed test server service.	<i>disable</i>	Disable speed test server service.									
	Option	Description														
	<i>enable</i>	Enable speed test server service.														
<i>disable</i>	Disable speed test server service.															
split-port *	Split port(s) to multiple 10Gbps ports.	string	Maximum length: 15													
ssd-trim-date *	Date within a month to run ssd trim.	integer	Minimum value: 1 1 Maximum value: 31													
ssd-trim-freq *	How often to run SSD Trim. SSD Trim prevents SSD drive data loss by finding and isolating errors.	option	-	weekly												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>never</i></td><td>Never Run SSD Trim.</td></tr><tr><td><i>hourly</i></td><td>Run SSD Trim Hourly.</td></tr><tr><td><i>daily</i></td><td>Run SSD Trim Daily.</td></tr><tr><td><i>weekly</i></td><td>Run SSD Trim Weekly.</td></tr><tr><td><i>monthly</i></td><td>Run SSD Trim Monthly.</td></tr></table>	Option	Description	<i>never</i>	Never Run SSD Trim.	<i>hourly</i>	Run SSD Trim Hourly.	<i>daily</i>	Run SSD Trim Daily.	<i>weekly</i>	Run SSD Trim Weekly.	<i>monthly</i>	Run SSD Trim Monthly.			
	Option	Description														
	<i>never</i>	Never Run SSD Trim.														
	<i>hourly</i>	Run SSD Trim Hourly.														
	<i>daily</i>	Run SSD Trim Daily.														
	<i>weekly</i>	Run SSD Trim Weekly.														
<i>monthly</i>	Run SSD Trim Monthly.															
ssd-trim-hour *	Hour of the day on which to run SSD Trim.	integer	Minimum value: 0 0 Maximum value: 23	1												
ssd-trim-min *	Minute of the hour on which to run SSD Trim.	integer	Minimum value: 0 0 Maximum value: 60	60												
ssd-trim-weekday *	Day of week to run SSD Trim.	option	-	sunday												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>sunday</i></td><td>Sunday</td></tr><tr><td><i>monday</i></td><td>Monday</td></tr><tr><td><i>tuesday</i></td><td>Tuesday</td></tr><tr><td><i>wednesday</i></td><td>Wednesday</td></tr><tr><td><i>thursday</i></td><td>Thursday</td></tr></table>	Option	Description	<i>sunday</i>	Sunday	<i>monday</i>	Monday	<i>tuesday</i>	Tuesday	<i>wednesday</i>	Wednesday	<i>thursday</i>	Thursday			
	Option	Description														
	<i>sunday</i>	Sunday														
	<i>monday</i>	Monday														
	<i>tuesday</i>	Tuesday														
	<i>wednesday</i>	Wednesday														
<i>thursday</i>	Thursday															

Parameter	Description	Type	Size	Default																																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>friday</td><td>Friday</td></tr><tr><td>saturday</td><td>Saturday</td></tr></table>	Option	Description	friday	Friday	saturday	Saturday																															
	Option	Description																																				
	friday	Friday																																				
saturday	Saturday																																					
ssh-enc-algo	Select one or more SSH ciphers.	option	-	chacha20-poly1305@openssh.com aes256-ctr aes256-gcm@openssh.com																																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>chacha20-poly1305@openssh.com</td><td>chacha20-poly1305@openssh.com</td></tr><tr><td>aes128-ctr</td><td>aes128-ctr</td></tr><tr><td>aes192-ctr</td><td>aes192-ctr</td></tr><tr><td>aes256-ctr</td><td>aes256-ctr</td></tr><tr><td>arcfour256</td><td>arcfour256</td></tr><tr><td>arcfour128</td><td>arcfour128</td></tr><tr><td>aes128-cbc</td><td>aes128-cbc</td></tr><tr><td>3des-cbc</td><td>3des-cbc</td></tr><tr><td>blowfish-cbc</td><td>blowfish-cbc</td></tr><tr><td>cast128-cbc</td><td>cast128-cbc</td></tr><tr><td>aes192-cbc</td><td>aes192-cbc</td></tr><tr><td>aes256-cbc</td><td>aes256-cbc</td></tr><tr><td>arcfour</td><td>arcfour</td></tr><tr><td>rijndael-cbc@lysator.liu.se</td><td>rijndael-cbc@lysator.liu.se</td></tr><tr><td>aes128-gcm@openssh.com</td><td>aes128-gcm@openssh.com</td></tr><tr><td>aes256-gcm@openssh.com</td><td>aes256-gcm@openssh.com</td></tr></table>	Option	Description	chacha20-poly1305@openssh.com	chacha20-poly1305@openssh.com	aes128-ctr	aes128-ctr	aes192-ctr	aes192-ctr	aes256-ctr	aes256-ctr	arcfour256	arcfour256	arcfour128	arcfour128	aes128-cbc	aes128-cbc	3des-cbc	3des-cbc	blowfish-cbc	blowfish-cbc	cast128-cbc	cast128-cbc	aes192-cbc	aes192-cbc	aes256-cbc	aes256-cbc	arcfour	arcfour	rijndael-cbc@lysator.liu.se	rijndael-cbc@lysator.liu.se	aes128-gcm@openssh.com	aes128-gcm@openssh.com	aes256-gcm@openssh.com	aes256-gcm@openssh.com			
	Option	Description																																				
	chacha20-poly1305@openssh.com	chacha20-poly1305@openssh.com																																				
	aes128-ctr	aes128-ctr																																				
	aes192-ctr	aes192-ctr																																				
	aes256-ctr	aes256-ctr																																				
	arcfour256	arcfour256																																				
	arcfour128	arcfour128																																				
	aes128-cbc	aes128-cbc																																				
	3des-cbc	3des-cbc																																				
	blowfish-cbc	blowfish-cbc																																				
	cast128-cbc	cast128-cbc																																				
	aes192-cbc	aes192-cbc																																				
	aes256-cbc	aes256-cbc																																				
	arcfour	arcfour																																				
	rijndael-cbc@lysator.liu.se	rijndael-cbc@lysator.liu.se																																				
	aes128-gcm@openssh.com	aes128-gcm@openssh.com																																				
aes256-gcm@openssh.com	aes256-gcm@openssh.com																																					
ssh-kex-algo	Select one or more SSH kex algorithms.	option	-	diffie-hellman-group-exchange-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521																																		



Parameter	Description	Type	Size	Default																				
		<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>diffie-hellman-group1-sha1</i></td><td>diffie-hellman-group1-sha1</td></tr><tr><td><i>diffie-hellman-group14-sha1</i></td><td>diffie-hellman-group14-sha1</td></tr><tr><td><i>diffie-hellman-group-exchange-sha1</i></td><td>diffie-hellman-group-exchange-sha1</td></tr><tr><td><i>diffie-hellman-group-exchange-sha256</i></td><td>diffie-hellman-group-exchange-sha256</td></tr><tr><td><i>curve25519-sha256@libssh.org</i></td><td>curve25519-sha256@libssh.org</td></tr><tr><td><i>ecdh-sha2-nistp256</i></td><td>ecdh-sha2-nistp256</td></tr><tr><td><i>ecdh-sha2-nistp384</i></td><td>ecdh-sha2-nistp384</td></tr><tr><td><i>ecdh-sha2-nistp521</i></td><td>ecdh-sha2-nistp521</td></tr></table>	Option	Description	<i>diffie-hellman-group1-sha1</i>	diffie-hellman-group1-sha1	<i>diffie-hellman-group14-sha1</i>	diffie-hellman-group14-sha1	<i>diffie-hellman-group-exchange-sha1</i>	diffie-hellman-group-exchange-sha1	<i>diffie-hellman-group-exchange-sha256</i>	diffie-hellman-group-exchange-sha256	<i>curve25519-sha256@libssh.org</i>	curve25519-sha256@libssh.org	<i>ecdh-sha2-nistp256</i>	ecdh-sha2-nistp256	<i>ecdh-sha2-nistp384</i>	ecdh-sha2-nistp384	<i>ecdh-sha2-nistp521</i>	ecdh-sha2-nistp521				
	Option	Description																						
	<i>diffie-hellman-group1-sha1</i>	diffie-hellman-group1-sha1																						
	<i>diffie-hellman-group14-sha1</i>	diffie-hellman-group14-sha1																						
	<i>diffie-hellman-group-exchange-sha1</i>	diffie-hellman-group-exchange-sha1																						
	<i>diffie-hellman-group-exchange-sha256</i>	diffie-hellman-group-exchange-sha256																						
	<i>curve25519-sha256@libssh.org</i>	curve25519-sha256@libssh.org																						
	<i>ecdh-sha2-nistp256</i>	ecdh-sha2-nistp256																						
<i>ecdh-sha2-nistp384</i>	ecdh-sha2-nistp384																							
<i>ecdh-sha2-nistp521</i>	ecdh-sha2-nistp521																							
ssh-mac-algo	Select one or more SSH MAC algorithms.	option	-	hmac-sha2-256 hmac-sha2-256-etm@openssh.com hmac-sha2-512 hmac-sha2-512-etm@openssh.com																				
		<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>hmac-md5</i></td><td>hmac-md5</td></tr><tr><td><i>hmac-md5-etm@openssh.com</i></td><td>hmac-md5-etm@openssh.com</td></tr><tr><td><i>hmac-md5-96</i></td><td>hmac-md5-96</td></tr><tr><td><i>hmac-md5-96-etm@openssh.com</i></td><td>hmac-md5-96-etm@openssh.com</td></tr><tr><td><i>hmac-sha1</i></td><td>hmac-sha1</td></tr><tr><td><i>hmac-sha1-etm@openssh.com</i></td><td>hmac-sha1-etm@openssh.com</td></tr><tr><td><i>hmac-sha2-256</i></td><td>hmac-sha2-256</td></tr><tr><td><i>hmac-sha2-256-etm@openssh.com</i></td><td>hmac-sha2-256-etm@openssh.com</td></tr><tr><td><i>hmac-sha2-512</i></td><td>hmac-sha2-512</td></tr></table>	Option	Description	<i>hmac-md5</i>	hmac-md5	<i>hmac-md5-etm@openssh.com</i>	hmac-md5-etm@openssh.com	<i>hmac-md5-96</i>	hmac-md5-96	<i>hmac-md5-96-etm@openssh.com</i>	hmac-md5-96-etm@openssh.com	<i>hmac-sha1</i>	hmac-sha1	<i>hmac-sha1-etm@openssh.com</i>	hmac-sha1-etm@openssh.com	<i>hmac-sha2-256</i>	hmac-sha2-256	<i>hmac-sha2-256-etm@openssh.com</i>	hmac-sha2-256-etm@openssh.com	<i>hmac-sha2-512</i>	hmac-sha2-512		
	Option	Description																						
	<i>hmac-md5</i>	hmac-md5																						
	<i>hmac-md5-etm@openssh.com</i>	hmac-md5-etm@openssh.com																						
	<i>hmac-md5-96</i>	hmac-md5-96																						
	<i>hmac-md5-96-etm@openssh.com</i>	hmac-md5-96-etm@openssh.com																						
	<i>hmac-sha1</i>	hmac-sha1																						
	<i>hmac-sha1-etm@openssh.com</i>	hmac-sha1-etm@openssh.com																						
	<i>hmac-sha2-256</i>	hmac-sha2-256																						
	<i>hmac-sha2-256-etm@openssh.com</i>	hmac-sha2-256-etm@openssh.com																						
<i>hmac-sha2-512</i>	hmac-sha2-512																							

Parameter	Description	Type	Size	Default																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>hmac-sha2-512-etm@openssh.com</i></td><td>hmac-sha2-512-etm@openssh.com</td></tr><tr><td><i>hmac-ripemd160</i></td><td>hmac-ripemd160</td></tr><tr><td><i>hmac-ripemd160@openssh.com</i></td><td>hmac-ripemd160@openssh.com</td></tr><tr><td><i>hmac-ripemd160-etm@openssh.com</i></td><td>hmac-ripemd160-etm@openssh.com</td></tr><tr><td><i>umac-64@openssh.com</i></td><td>umac-64@openssh.com</td></tr><tr><td><i>umac-128@openssh.com</i></td><td>umac-128@openssh.com</td></tr><tr><td><i>umac-64-etm@openssh.com</i></td><td>umac-64-etm@openssh.com</td></tr><tr><td><i>umac-128-etm@openssh.com</i></td><td>umac-128-etm@openssh.com</td></tr></table>	Option	Description	<i>hmac-sha2-512-etm@openssh.com</i>	hmac-sha2-512-etm@openssh.com	<i>hmac-ripemd160</i>	hmac-ripemd160	<i>hmac-ripemd160@openssh.com</i>	hmac-ripemd160@openssh.com	<i>hmac-ripemd160-etm@openssh.com</i>	hmac-ripemd160-etm@openssh.com	<i>umac-64@openssh.com</i>	umac-64@openssh.com	<i>umac-128@openssh.com</i>	umac-128@openssh.com	<i>umac-64-etm@openssh.com</i>	umac-64-etm@openssh.com	<i>umac-128-etm@openssh.com</i>	umac-128-etm@openssh.com			
	Option	Description																				
	<i>hmac-sha2-512-etm@openssh.com</i>	hmac-sha2-512-etm@openssh.com																				
	<i>hmac-ripemd160</i>	hmac-ripemd160																				
	<i>hmac-ripemd160@openssh.com</i>	hmac-ripemd160@openssh.com																				
	<i>hmac-ripemd160-etm@openssh.com</i>	hmac-ripemd160-etm@openssh.com																				
	<i>umac-64@openssh.com</i>	umac-64@openssh.com																				
	<i>umac-128@openssh.com</i>	umac-128@openssh.com																				
	<i>umac-64-etm@openssh.com</i>	umac-64-etm@openssh.com																				
<i>umac-128-etm@openssh.com</i>	umac-128-etm@openssh.com																					
ssl-min-proto-version	Minimum supported protocol version for SSL/TLS connections.	option	-	TLSv1-2																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>SSLv3</i></td><td>SSLv3.</td></tr><tr><td><i>TLSv1</i></td><td>TLSv1.</td></tr><tr><td><i>TLSv1-1</i></td><td>TLSv1.1.</td></tr><tr><td><i>TLSv1-2</i></td><td>TLSv1.2.</td></tr><tr><td><i>TLSv1-3</i></td><td>TLSv1.3.</td></tr></table>	Option	Description	<i>SSLv3</i>	SSLv3.	<i>TLSv1</i>	TLSv1.	<i>TLSv1-1</i>	TLSv1.1.	<i>TLSv1-2</i>	TLSv1.2.	<i>TLSv1-3</i>	TLSv1.3.									
	Option	Description																				
	<i>SSLv3</i>	SSLv3.																				
	<i>TLSv1</i>	TLSv1.																				
	<i>TLSv1-1</i>	TLSv1.1.																				
	<i>TLSv1-2</i>	TLSv1.2.																				
<i>TLSv1-3</i>	TLSv1.3.																					
ssl-static-key-ciphers	Enable/disable static key ciphers in SSL/TLS connections (e.g. AES128-SHA, AES256-SHA, AES128-SHA256, AES256-SHA256).	option	-	enable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable static key ciphers in SSL/TLS connections.</td></tr><tr><td><i>disable</i></td><td>Disable static key ciphers in SSL/TLS connections.</td></tr></table>	Option	Description	<i>enable</i>	Enable static key ciphers in SSL/TLS connections.	<i>disable</i>	Disable static key ciphers in SSL/TLS connections.															
	Option	Description																				
	<i>enable</i>	Enable static key ciphers in SSL/TLS connections.																				
<i>disable</i>	Disable static key ciphers in SSL/TLS connections.																					

Parameter	Description	Type	Size	Default						
sslvpn-cipher-hardware-acceleration *	Enable/disable SSL-VPN hardware acceleration.	option	-	disable **						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable SSL-VPN cipher hardware acceleration.</td></tr><tr><td><i>disable</i></td><td>Disable SSL-VPN cipher hardware acceleration.</td></tr></table>	Option	Description	<i>enable</i>	Enable SSL-VPN cipher hardware acceleration.	<i>disable</i>	Disable SSL-VPN cipher hardware acceleration.			
Option	Description									
<i>enable</i>	Enable SSL-VPN cipher hardware acceleration.									
<i>disable</i>	Disable SSL-VPN cipher hardware acceleration.									
sslvpn-ems-sn-check	Enable/disable verification of EMS serial number in SSL-VPN connection.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable verification of EMS serial number in SSL-VPN connection.</td></tr><tr><td><i>disable</i></td><td>Disable verification of EMS serial number in SSL-VPN connection.</td></tr></table>	Option	Description	<i>enable</i>	Enable verification of EMS serial number in SSL-VPN connection.	<i>disable</i>	Disable verification of EMS serial number in SSL-VPN connection.			
Option	Description									
<i>enable</i>	Enable verification of EMS serial number in SSL-VPN connection.									
<i>disable</i>	Disable verification of EMS serial number in SSL-VPN connection.									
sslvpn-kxp-hardware-acceleration *	Enable/disable SSL-VPN KXP hardware acceleration.	option	-	disable **						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable KXP SSL-VPN hardware acceleration.</td></tr><tr><td><i>disable</i></td><td>Disable KXP SSL-VPN hardware acceleration.</td></tr></table>	Option	Description	<i>enable</i>	Enable KXP SSL-VPN hardware acceleration.	<i>disable</i>	Disable KXP SSL-VPN hardware acceleration.			
Option	Description									
<i>enable</i>	Enable KXP SSL-VPN hardware acceleration.									
<i>disable</i>	Disable KXP SSL-VPN hardware acceleration.									
sslvpn-max-worker-count	Maximum number of SSL-VPN processes. Upper limit for this value is the number of CPUs and depends on the model. Default value of zero means the SSLVPN daemon decides the number of worker processes.	integer	Minimum value: 0 0 Maximum value: 8 **							
sslvpn-plugin-version-check	Enable/disable checking browser's plugin version by SSL-VPN.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable SSL-VPN automatic checking of browser plug-in version.</td></tr><tr><td><i>disable</i></td><td>Disable SSL-VPN automatic checking of browser plug-in version.</td></tr></table>	Option	Description	<i>enable</i>	Enable SSL-VPN automatic checking of browser plug-in version.	<i>disable</i>	Disable SSL-VPN automatic checking of browser plug-in version.			
Option	Description									
<i>enable</i>	Enable SSL-VPN automatic checking of browser plug-in version.									
<i>disable</i>	Disable SSL-VPN automatic checking of browser plug-in version.									

Parameter	Description	Type	Size	Default						
strict-dirty-session-check	Enable to check the session against the original policy when revalidating. This can prevent dropping of redirected sessions when web-filtering and authentication are enabled together. If this option is enabled, the FortiGate unit deletes a session if a routing or policy change causes the session to no longer match the policy that originally allowed the session.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable strict dirty-session check.</td></tr><tr><td><i>disable</i></td><td>Disable strict dirty-session check.</td></tr></table>	Option	Description	<i>enable</i>	Enable strict dirty-session check.	<i>disable</i>	Disable strict dirty-session check.			
Option	Description									
<i>enable</i>	Enable strict dirty-session check.									
<i>disable</i>	Disable strict dirty-session check.									
strong-crypto	Enable to use strong encryption and only allow strong ciphers and digest for HTTPS/SSH/TLS/SSL functions.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable strong crypto for HTTPS/SSH/TLS/SSL.</td></tr><tr><td><i>disable</i></td><td>Disable strong crypto for HTTPS/SSH/TLS/SSL.</td></tr></table>	Option	Description	<i>enable</i>	Enable strong crypto for HTTPS/SSH/TLS/SSL.	<i>disable</i>	Disable strong crypto for HTTPS/SSH/TLS/SSL.			
Option	Description									
<i>enable</i>	Enable strong crypto for HTTPS/SSH/TLS/SSL.									
<i>disable</i>	Disable strong crypto for HTTPS/SSH/TLS/SSL.									
switch-controller *	Enable/disable switch controller feature. Switch controller allows you to manage FortiSwitch from the FortiGate itself.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable switch controller feature.</td></tr><tr><td><i>enable</i></td><td>Enable switch controller feature.</td></tr></table>	Option	Description	<i>disable</i>	Disable switch controller feature.	<i>enable</i>	Enable switch controller feature.			
Option	Description									
<i>disable</i>	Disable switch controller feature.									
<i>enable</i>	Enable switch controller feature.									

Parameter	Description	Type	Size	Default
switch-controller-reserved-network *	Configure reserved network subnet for managed switches. This is available when the switch controller is enabled.	ipv4-classnet-host	Not Specified	10.255.0.0 255.255.0.0
sys-perf-log-interval	Time in minutes between updates of performance statistics logging..	integer	Minimum value: 0 Maximum value: 15	5
tcp-halfclose-timer	Number of seconds the FortiGate unit should wait to close a session after one peer has sent a FIN packet but the other has not responded.	integer	Minimum value: 1 Maximum value: 86400	120
tcp-halfopen-timer	Number of seconds the FortiGate unit should wait to close a session after one peer has sent an open session packet but the other has not responded.	integer	Minimum value: 1 Maximum value: 86400	10
tcp-option	Enable SACK, timestamp and MSS TCP options.	option	-	enable
	Option	Description		
	enable	Enable TCP option.		
	disable	Disable TCP option.		
tcp-rst-timer	Length of the TCP CLOSE state in seconds.	integer	Minimum value: 5 Maximum value: 300	5
tcp-timewait-timer	Length of the TCP TIME-WAIT state in seconds.	integer	Minimum value: 0 Maximum value: 300	1
tftp	Enable/disable TFTP.	option	-	enable
	Option	Description		
	enable	Enable TFTP.		
	disable	Disable TFTP.		

Parameter	Description	Type	Size	Default
timezone	Number corresponding to your time zone from 00 to 86. Enter set timezone ? to view the list of time zones and the numbers that represent them.	option	-	00

Option	Description
01	(GMT-11:00) Midway Island, Samoa
02	(GMT-10:00) Hawaii
03	(GMT-9:00) Alaska
04	(GMT-8:00) Pacific Time (US & Canada)
05	(GMT-7:00) Arizona
81	(GMT-7:00) Baja California Sur, Chihuahua
06	(GMT-7:00) Mountain Time (US & Canada)
07	(GMT-6:00) Central America
08	(GMT-6:00) Central Time (US & Canada)
09	(GMT-6:00) Mexico City
10	(GMT-6:00) Saskatchewan
11	(GMT-5:00) Bogota, Lima, Quito
12	(GMT-5:00) Eastern Time (US & Canada)
13	(GMT-5:00) Indiana (East)
74	(GMT-4:00) Caracas
14	(GMT-4:00) Atlantic Time (Canada)
77	(GMT-4:00) Georgetown
15	(GMT-4:00) La Paz
87	(GMT-4:00) Paraguay
16	(GMT-3:00) Santiago
17	(GMT-3:30) Newfoundland
18	(GMT-3:00) Brasilia
19	(GMT-3:00) Buenos Aires
20	(GMT-3:00) Nuuk (Greenland)

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	75	(GMT-3:00) Uruguay		
	21	(GMT-2:00) Mid-Atlantic		
	22	(GMT-1:00) Azores		
	23	(GMT-1:00) Cape Verde Is.		
	24	(GMT) Monrovia		
	80	(GMT) Greenwich Mean Time		
	79	(GMT) Casablanca		
	25	(GMT) Dublin, Edinburgh, Lisbon, London, Canary Is.		
	26	(GMT+1:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna		
	27	(GMT+1:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague		
	28	(GMT+1:00) Brussels, Copenhagen, Madrid, Paris		
	78	(GMT+1:00) Namibia		
	29	(GMT+1:00) Sarajevo, Skopje, Warsaw, Zagreb		
	30	(GMT+1:00) West Central Africa		
	31	(GMT+2:00) Athens, Sofia, Vilnius		
	32	(GMT+2:00) Bucharest		
	33	(GMT+2:00) Cairo		
	34	(GMT+2:00) Harare, Pretoria		
	35	(GMT+2:00) Helsinki, Riga, Tallinn		
	36	(GMT+2:00) Jerusalem		
	37	(GMT+3:00) Baghdad		
	38	(GMT+3:00) Kuwait, Riyadh		
	83	(GMT+3:00) Moscow		
	84	(GMT+3:00) Minsk		
	40	(GMT+3:00) Nairobi		
	85	(GMT+3:00) Istanbul		
	41	(GMT+3:30) Tehran		
	42	(GMT+4:00) Abu Dhabi, Muscat		
	43	(GMT+4:00) Baku		

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	39	(GMT+3:00) St. Petersburg, Volgograd		
	44	(GMT+4:30) Kabul		
	46	(GMT+5:00) Islamabad, Karachi, Tashkent		
	47	(GMT+5:30) Kolkata, Chennai, Mumbai, New Delhi		
	51	(GMT+5:30) Sri Jayawardenepara		
	48	(GMT+5:45) Kathmandu		
	45	(GMT+5:00) Ekaterinburg		
	49	(GMT+6:00) Almaty, Novosibirsk		
	50	(GMT+6:00) Astana, Dhaka		
	52	(GMT+6:30) Rangoon		
	53	(GMT+7:00) Bangkok, Hanoi, Jakarta		
	54	(GMT+7:00) Krasnoyarsk		
	55	(GMT+8:00) Beijing, ChongQing, HongKong, Urumgi, Irkutsk		
	56	(GMT+8:00) Ulaan Bataar		
	57	(GMT+8:00) Kuala Lumpur, Singapore		
	58	(GMT+8:00) Perth		
	59	(GMT+8:00) Taipei		
	60	(GMT+9:00) Osaka, Sapporo, Tokyo, Seoul		
	62	(GMT+9:30) Adelaide		
	63	(GMT+9:30) Darwin		
	61	(GMT+9:00) Yakutsk		
	64	(GMT+10:00) Brisbane		
	65	(GMT+10:00) Canberra, Melbourne, Sydney		
	66	(GMT+10:00) Guam, Port Moresby		
	67	(GMT+10:00) Hobart		
	68	(GMT+10:00) Vladivostok		
	69	(GMT+10:00) Magadan		
	70	(GMT+11:00) Solomon Is., New Caledonia		
	71	(GMT+12:00) Auckland, Wellington		



Parameter	Description	Type	Size	Default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>72</td><td>(GMT+12:00) Fiji, Kamchatka, Marshall Is.</td></tr><tr><td>00</td><td>(GMT+12:00) Eniwetok, Kwajalein</td></tr><tr><td>82</td><td>(GMT+12:45) Chatham Islands</td></tr><tr><td>73</td><td>(GMT+13:00) Nuku'alofa</td></tr><tr><td>86</td><td>(GMT+13:00) Samoa</td></tr><tr><td>76</td><td>(GMT+14:00) Kiritimati</td></tr></table>				Option	Description	72	(GMT+12:00) Fiji, Kamchatka, Marshall Is.	00	(GMT+12:00) Eniwetok, Kwajalein	82	(GMT+12:45) Chatham Islands	73	(GMT+13:00) Nuku'alofa	86	(GMT+13:00) Samoa	76	(GMT+14:00) Kiritimati
	Option	Description																
	72	(GMT+12:00) Fiji, Kamchatka, Marshall Is.																
	00	(GMT+12:00) Eniwetok, Kwajalein																
	82	(GMT+12:45) Chatham Islands																
	73	(GMT+13:00) Nuku'alofa																
	86	(GMT+13:00) Samoa																
76	(GMT+14:00) Kiritimati																	
traffic-priority	Choose Type of Service (ToS) or Differentiated Services Code Point (DSCP) for traffic prioritization in traffic shaping.	option	-	tos														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>tos</td><td>IP TOS.</td></tr><tr><td>dscp</td><td>DSCP (DiffServ) DS.</td></tr></table>				Option	Description	tos	IP TOS.	dscp	DSCP (DiffServ) DS.								
	Option	Description																
	tos	IP TOS.																
dscp	DSCP (DiffServ) DS.																	
traffic-priority-level	Default system-wide level of priority for traffic prioritization.	option	-	medium														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>low</td><td>Low priority.</td></tr><tr><td>medium</td><td>Medium priority.</td></tr><tr><td>high</td><td>High priority.</td></tr></table>				Option	Description	low	Low priority.	medium	Medium priority.	high	High priority.						
	Option	Description																
	low	Low priority.																
	medium	Medium priority.																
high	High priority.																	
two-factor-email-expiry	Email-based two-factor authentication session timeout.	integer	Minimum value: 30 Maximum value: 300	60														
two-factor-fac-expiry	FortiAuthenticator token authentication session timeout.	integer	Minimum value: 10 Maximum value: 3600	60														
two-factor-ftk-expiry	FortiToken authentication session timeout.	integer	Minimum value: 60 Maximum value: 600	60														

Parameter	Description	Type	Size	Default								
two-factor-ftm-expiry	FortiToken Mobile session timeout.	integer	Minimum value: 1 Maximum value: 168	72								
two-factor-sms-expiry	SMS-based two-factor authentication session timeout.	integer	Minimum value: 30 Maximum value: 300	60								
udp-idle-timer	UDP connection session timeout. This command can be useful in managing CPU and memory resources.	integer	Minimum value: 1 Maximum value: 86400	180								
url-filter-affinity *	URL filter CPU affinity.	string	Maximum length: 79	0								
url-filter-count	URL filter daemon count.	integer	Minimum value: 1 Maximum value: 1 **	1								
user-device-store-max-devices	Maximum number of devices allowed in user device store.	integer	Minimum value: 84220 Maximum value: 240629 **	168440 **								
user-device-store-max-unified-mem	Maximum unified memory allowed in user device store.	integer	Minimum value: 168440954 Maximum value: 1684409548 **	842204774 **								
user-device-store-max-users	Maximum number of users allowed in user device store.	integer	Minimum value: 84220 Maximum value: 240629 **	168440 **								
user-server-cert	Certificate to use for https user authentication.	string	Maximum length: 35	Fortinet_Factory								
vdom-mode *	Enable/disable support for split/multiple virtual domains (VDOMs).	option	-	no-vdom								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>no-vdom</td><td>Disable split/multiple VDOMs mode.</td></tr><tr><td>split-vdom</td><td>Enable split VDOMs mode.</td></tr><tr><td>multi-vdom</td><td>Enable multiple VDOMs mode.</td></tr></table>				Option	Description	no-vdom	Disable split/multiple VDOMs mode.	split-vdom	Enable split VDOMs mode.	multi-vdom	Enable multiple VDOMs mode.
Option	Description											
no-vdom	Disable split/multiple VDOMs mode.											
split-vdom	Enable split VDOMs mode.											
multi-vdom	Enable multiple VDOMs mode.											

Parameter	Description	Type	Size	Default						
vip-arp-range	Controls the number of ARPs that the FortiGate sends for a Virtual IP (VIP) address range.	option	-	restricted						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>unlimited</i></td><td>Send ARPs for all addresses in VIP range.</td></tr><tr><td><i>restricted</i></td><td>Send ARPs for the first 8192 addresses in VIP range.</td></tr></table>	Option	Description	<i>unlimited</i>	Send ARPs for all addresses in VIP range.	<i>restricted</i>	Send ARPs for the first 8192 addresses in VIP range.			
Option	Description									
<i>unlimited</i>	Send ARPs for all addresses in VIP range.									
<i>restricted</i>	Send ARPs for the first 8192 addresses in VIP range.									
virtual-switch-vlan *	Enable/disable virtual switch VLAN.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable virtual switch VLAN.</td></tr><tr><td><i>disable</i></td><td>Disable virtual switch VLAN.</td></tr></table>	Option	Description	<i>enable</i>	Enable virtual switch VLAN.	<i>disable</i>	Disable virtual switch VLAN.			
Option	Description									
<i>enable</i>	Enable virtual switch VLAN.									
<i>disable</i>	Disable virtual switch VLAN.									
wad-affinity *	Affinity setting for wad (hexadecimal value up to 256 bits in the format of xxxxxxxxxxxxxxxxx).	string	Maximum length: 79	0						
wad-csvc-cs-count	Number of concurrent WAD-cache-service object-cache processes.	integer	Minimum value: 1 Maximum value: 1	1						
wad-csvc-db-count	Number of concurrent WAD-cache-service byte-cache processes.	integer	Minimum value: 0 Maximum value: 8 **	0						
wad-memory-change-granularity	Minimum percentage change in system memory usage detected by the wad daemon prior to adjusting TCP window size for any active connection.	integer	Minimum value: 5 Maximum value: 25	10						
wad-source-affinity	Enable/disable dispatching traffic to WAD workers based on source affinity.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable dispatching traffic to WAD workers based on source affinity.</td></tr><tr><td><i>enable</i></td><td>Enable dispatching traffic to WAD workers based on source affinity.</td></tr></table>	Option	Description	<i>disable</i>	Disable dispatching traffic to WAD workers based on source affinity.	<i>enable</i>	Enable dispatching traffic to WAD workers based on source affinity.			
Option	Description									
<i>disable</i>	Disable dispatching traffic to WAD workers based on source affinity.									
<i>enable</i>	Enable dispatching traffic to WAD workers based on source affinity.									

Parameter	Description	Type	Size	Default								
wad-worker-count	Number of explicit proxy WAN optimization daemon (WAD) processes. By default WAN optimization, explicit proxy, and web caching is handled by all of the CPU cores in a FortiGate unit.	integer	Minimum value: 0 Maximum value: 8 **	0								
wifi-ca-certificate	CA certificate that verifies the WiFi certificate.	string	Maximum length: 79	Fortinet_Wifi_CA								
wifi-certificate	Certificate to use for WiFi authentication.	string	Maximum length: 35	Fortinet_Wifi								
wimax-4g-usb	Enable/disable comparability with WiMAX 4G USB devices.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable WiMax 4G.</td></tr><tr><td><i>disable</i></td><td>Disable WiMax 4G.</td></tr></table>				Option	Description	<i>enable</i>	Enable WiMax 4G.	<i>disable</i>	Disable WiMax 4G.		
Option	Description											
<i>enable</i>	Enable WiMax 4G.											
<i>disable</i>	Disable WiMax 4G.											
wireless-controller	Enable/disable the wireless controller feature to use the FortiGate unit to manage FortiAPs.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable wireless controller.</td></tr><tr><td><i>disable</i></td><td>Disable wireless controller.</td></tr></table>				Option	Description	<i>enable</i>	Enable wireless controller.	<i>disable</i>	Disable wireless controller.		
Option	Description											
<i>enable</i>	Enable wireless controller.											
<i>disable</i>	Disable wireless controller.											
wireless-controller-port	Port used for the control channel in wireless controller mode.	integer	Minimum value: 1024 Maximum value: 49150	5246								
wireless-mode *	Wireless mode setting.	option	-	ac								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ac</i></td><td>Wireless controller with local wireless.</td></tr><tr><td><i>client</i></td><td>Wireless client mode.</td></tr><tr><td><i>fwfap</i></td><td>Obsolete wireless AP mode.</td></tr></table>				Option	Description	<i>ac</i>	Wireless controller with local wireless.	<i>client</i>	Wireless client mode.	<i>fwfap</i>	Obsolete wireless AP mode.
Option	Description											
<i>ac</i>	Wireless controller with local wireless.											
<i>client</i>	Wireless client mode.											
<i>fwfap</i>	Obsolete wireless AP mode.											

\* This parameter may not exist in some models.

\*\* Values may differ between models.

## config split-port-mode

Parameter	Description	Type	Size	Default
interface	Split port interface.	string	Maximum length: 15	
split-mode	The configuration mode for the split port interface.	option	-	disable
		Option	Description	
		<i>disable</i>	Disable split.	
		<i>4x10G</i>	Split the port into four 10G ports.	
		<i>4x25G</i>	Split the port into four 25G ports.	
		<i>8x25G</i>	Split the port into eight 25G ports.	
		<i>8x50G</i>	Split the port into eight 50G ports.	
		<i>4x100G</i>	Split the port into four 100G ports.	

## config system gre-tunnel

Configure GRE tunnel.

```
config system gre-tunnel
  Description: Configure GRE tunnel.
  edit <name>
    set auto-asic-offload [enable|disable]
    set checksum-reception [disable|enable]
    set checksum-transmission [disable|enable]
    set diffservcode {user}
    set dscp-copying [disable|enable]
    set interface {string}
    set ip-version [4|6]
    set keepalive-failtimes {integer}
    set keepalive-interval {integer}
    set key-inbound {integer}
    set key-outbound {integer}
    set local-gw {ipv4-address-any}
    set local-gw6 {ipv6-address}
    set remote-gw {ipv4-address}
    set remote-gw6 {ipv6-address}
    set sequence-number-reception [disable|enable]
    set sequence-number-transmission [disable|enable]
    set use-sdwan [disable|enable]
  next
end
```

## config system gre-tunnel

Parameter	Description	Type	Size	Default						
auto-asic-offload *	Enable/disable automatic ASIC offloading.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable automatic ASIC offloading.</td></tr><tr><td>disable</td><td>Disable automatic ASIC offloading.</td></tr></table>	Option	Description	enable	Enable automatic ASIC offloading.	disable	Disable automatic ASIC offloading.			
Option	Description									
enable	Enable automatic ASIC offloading.									
disable	Disable automatic ASIC offloading.									
checksum-reception *	Enable/disable validating checksums in received GRE packets.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Do not validate checksums in received GRE packets.</td></tr><tr><td>enable</td><td>Validate checksums in received GRE packets.</td></tr></table>	Option	Description	disable	Do not validate checksums in received GRE packets.	enable	Validate checksums in received GRE packets.			
Option	Description									
disable	Do not validate checksums in received GRE packets.									
enable	Validate checksums in received GRE packets.									
checksum-transmission *	Enable/disable including checksums in transmitted GRE packets.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Do not include checksums in transmitted GRE packets.</td></tr><tr><td>enable</td><td>Include checksums in transmitted GRE packets.</td></tr></table>	Option	Description	disable	Do not include checksums in transmitted GRE packets.	enable	Include checksums in transmitted GRE packets.			
Option	Description									
disable	Do not include checksums in transmitted GRE packets.									
enable	Include checksums in transmitted GRE packets.									
diffservcode	DiffServ setting to be applied to GRE tunnel outer IP header.	user	Not Specified							
dscp-copying	Enable/disable DSCP copying.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable DSCP copying.</td></tr><tr><td>enable</td><td>Enable DSCP copying.</td></tr></table>	Option	Description	disable	Disable DSCP copying.	enable	Enable DSCP copying.			
Option	Description									
disable	Disable DSCP copying.									
enable	Enable DSCP copying.									
interface	Interface name.	string	Maximum length: 15							
ip-version	IP version to use for VPN interface.	option	-	4						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>4</td><td>Use IPv4 addressing for gateways.</td></tr><tr><td>6</td><td>Use IPv6 addressing for gateways.</td></tr></table>	Option	Description	4	Use IPv4 addressing for gateways.	6	Use IPv6 addressing for gateways.			
Option	Description									
4	Use IPv4 addressing for gateways.									
6	Use IPv6 addressing for gateways.									

Parameter	Description	Type	Size	Default						
keepalive-failtimes	Number of consecutive unreturned keepalive messages before a GRE connection is considered down.	integer	Minimum value: 1 Maximum value: 255	10						
keepalive-interval	Keepalive message interval.	integer	Minimum value: 0 Maximum value: 32767	0						
key-inbound *	Require received GRE packets contain this key.	integer	Minimum value: 0 Maximum value: 4294967295	0						
key-outbound *	Include this key in transmitted GRE packets.	integer	Minimum value: 0 Maximum value: 4294967295	0						
local-gw	IP address of the local gateway.	ipv4-address-any	Not Specified	0.0.0.0						
local-gw6	IPv6 address of the local gateway.	ipv6-address	Not Specified	::						
name	Tunnel name.	string	Maximum length: 15							
remote-gw	IP address of the remote gateway.	ipv4-address	Not Specified	0.0.0.0						
remote-gw6	IPv6 address of the remote gateway.	ipv6-address	Not Specified	::						
sequence-number-reception *	Enable/disable validating sequence numbers in received GRE packets.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Do not validate sequence number in received GRE packets.</td></tr><tr><td>enable</td><td>Validate sequence numbers in received GRE packets.</td></tr></table>				Option	Description	disable	Do not validate sequence number in received GRE packets.	enable	Validate sequence numbers in received GRE packets.
Option	Description									
disable	Do not validate sequence number in received GRE packets.									
enable	Validate sequence numbers in received GRE packets.									
sequence-number-transmission *	Enable/disable including of sequence numbers in transmitted GRE packets.	option	-	disable						

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Include sequence numbers in transmitted GRE packets.		
	<i>enable</i>	Do not include sequence numbers in transmitted GRE packets.		
use-sdwan	Enable/disable use of SD-WAN to reach remote gateway.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable use of SD-WAN to reach remote gateway.		
	<i>enable</i>	Enable use of SD-WAN to reach remote gateway.		

\* This parameter may not exist in some models.

## config system ha-monitor

Configure HA monitor.

```
config system ha-monitor
    Description: Configure HA monitor.
    set monitor-vlan [enable|disable]
    set vlan-hb-interval {integer}
    set vlan-hb-lost-threshold {integer}
end
```

## config system ha-monitor

Parameter	Description	Type	Size	Default
monitor-vlan	Enable/disable monitor VLAN interfaces.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable monitor VLAN interfaces.		
	<i>disable</i>	Disable monitor VLAN interfaces.		
vlan-hb-interval	Configure heartbeat interval (seconds).	integer	Minimum value: 1 Maximum value: 30	5
vlan-hb-lost-threshold	VLAN lost heartbeat threshold.	integer	Minimum value: 1 Maximum value: 60	3



---

## config system ha

Configure HA.

```
config system ha
    Description: Configure HA.
    set arps {integer}
    set arps-interval {integer}
    set authentication [enable|disable]
    set cpu-threshold {user}
    set encryption [enable|disable]
    set failover-hold-time {integer}
    set ftp-proxy-threshold {user}
    set gratuitous-arps [enable|disable]
    set group-id {integer}
    set group-name {string}
    set ha-direct [enable|disable]
    set ha-eth-type {string}
    config ha-mgmt-interfaces
        Description: Reserve interfaces to manage individual cluster units.
        edit <id>
            set interface {string}
            set dst {ipv4-classnet}
            set gateway {ipv4-address}
            set gateway6 {ipv6-address}
        next
    end
    set ha-mgmt-status [enable|disable]
    set ha-uptime-diff-margin {integer}
    set hb-interval {integer}
    set hb-interval-in-milliseconds [100ms|10ms]
    set hb-lost-threshold {integer}
    set hbdev {user}
    set hc-eth-type {string}
    set hello-holddown {integer}
    set http-proxy-threshold {user}
    set hw-session-hold-time {integer}
    set hw-session-sync-delay {integer}
    set hw-session-sync-dev {string}
    set imap-proxy-threshold {user}
    set key {password}
    set l2ep-eth-type {string}
    set link-failed-signal [enable|disable]
    set load-balance-all [enable|disable]
    set logical-sn [enable|disable]
    set memory-based-failover [enable|disable]
    set memory-compatible-mode [enable|disable]
    set memory-failover-flip-timeout {integer}
    set memory-failover-monitor-period {integer}
    set memory-failover-sample-rate {integer}
    set memory-failover-threshold {integer}
    set memory-threshold {user}
    set mode [standalone|a-a|...]
    set monitor {user}
    set multicast-ttl {integer}
    set nntp-proxy-threshold {user}
```

```

set override [enable|disable]
set override-wait-time {integer}
set password {password}
set pingserver-failover-threshold {integer}
set pingserver-flip-timeout {integer}
set pingserver-monitor-interface {user}
set pingserver-secondary-force-reset [enable|disable]
set pop3-proxy-threshold {user}
set priority {integer}
set route-hold {integer}
set route-ttl {integer}
set route-wait {integer}
set schedule [none|hub|...]
config secondary-vcluster
    Description: Configure virtual cluster 2.
    set vcluster-id {integer}
    set override [enable|disable]
    set priority {integer}
    set override-wait-time {integer}
    set monitor {user}
    set pingserver-monitor-interface {user}
    set pingserver-failover-threshold {integer}
    set pingserver-secondary-force-reset [enable|disable]
    set vdom {user}
end
set session-pickup [enable|disable]
set session-pickup-connectionless [enable|disable]
set session-pickup-delay [enable|disable]
set session-pickup-expectation [enable|disable]
set session-pickup-nat [enable|disable]
set session-sync-dev {user}
set smtp-proxy-threshold {user}
set ssd-failover [enable|disable]
set standalone-config-sync [enable|disable]
set standalone-mgmt-vdom [enable|disable]
set sync-config [enable|disable]
set sync-packet-balance [enable|disable]
set unicast-gateway {ipv4-address}
set unicast-hb [enable|disable]
set unicast-hb-netmask {ipv4-netmask}
set unicast-hb-peerip {ipv4-address}
config unicast-peers
    Description: Number of unicast peers.
    edit <id>
        set peer-ip {ipv4-address}
    next
end
set unicast-status [enable|disable]
set uninterruptible-primary-wait {integer}
set uninterruptible-upgrade [enable|disable]
set vcluster-id {integer}
set vcluster2 [enable|disable]
set vdom {user}
set weight {user}
end

```

## config system ha

Parameter	Description	Type	Size	Default
arps	Number of gratuitous ARPs. Lower to reduce traffic. Higher to reduce failover time.	integer	Minimum value: 1 Maximum value: 60	5
arps-interval	Time between gratuitous ARPs . Lower to reduce failover time. Higher to reduce traffic.	integer	Minimum value: 1 Maximum value: 20	8
authentication	Enable/disable heartbeat message authentication.	option	-	disable
	Option	Description		
	enable	Enable heartbeat message authentication.		
	disable	Disable heartbeat message authentication.		
cpu-threshold	Dynamic weighted load balancing CPU usage weight and high and low thresholds.	user	Not Specified	
encryption	Enable/disable heartbeat message encryption.	option	-	disable
	Option	Description		
	enable	Enable heartbeat message encryption.		
	disable	Disable heartbeat message encryption.		
failover-hold-time	Time to wait before failover , to avoid flip.	integer	Minimum value: 0 Maximum value: 300	0
ftp-proxy-threshold	Dynamic weighted load balancing weight and high and low number of FTP proxy sessions.	user	Not Specified	
gratuitous-arps	Enable/disable gratuitous ARPs. Disable if link-failed-signal enabled.	option	-	enable
	Option	Description		
	enable	Enable gratuitous ARPs.		
	disable	Disable gratuitous ARPs.		

Parameter	Description	Type	Size	Default
group-id	HA group ID . Must be the same for all members.	integer	Minimum value: 0 Maximum value: 1023	0
group-name	Cluster group name. Must be the same for all members.	string	Maximum length: 32	
ha-direct	Enable/disable using ha-mgmt interface for syslog, SNMP, remote authentication (RADIUS), FortiAnalyzer, FortiSandbox, sFlow, and Netflow.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable using ha-mgmt interface for syslog, SNMP, remote authentication (RADIUS), FortiAnalyzer, FortiSandbox, sFlow, and Netflow.		
	<i>disable</i>	Disable using ha-mgmt interface for syslog, SNMP, remote authentication (RADIUS), FortiAnalyzer, FortiSandbox, sFlow, and Netflow.		
ha-eth-type	HA heartbeat packet Ethertype (4-digit hex).	string	Maximum length: 4	8890
ha-mgmt-status	Enable to reserve interfaces to manage individual cluster units.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
ha-uptime-diff-margin	Normally you would only reduce this value for failover testing.	integer	Minimum value: 1 Maximum value: 65535	300
hb-interval	Time between sending heartbeat packets. Increase to reduce false positives.	integer	Minimum value: 1 Maximum value: 20	2
hb-interval-in-milliseconds	Number of milliseconds for each heartbeat interval: 100ms or 10ms.	option	-	100ms
	<b>Option</b>	<b>Description</b>		
	<i>100ms</i>	Each heartbeat interval is 100ms.		
	<i>10ms</i>	Each heartbeat interval is 10ms.		

Parameter	Description	Type	Size	Default						
hb-lost-threshold	Number of lost heartbeats to signal a failure. Increase to reduce false positives.	integer	Minimum value: 1 Maximum value: 60	6 **						
hbdev	Heartbeat interfaces. Must be the same for all members. Enter <interface> <priority> pairs to specify the priority of each heartbeat interface. Higher priority takes precedence.	user	Not Specified							
hc-eth-type	Transparent mode HA heartbeat packet Ethertype (4-digit hex).	string	Maximum length: 4	8891						
hello-holddown	Time to wait before changing from hello to work state.	integer	Minimum value: 5 Maximum value: 300	20						
http-proxy-threshold	Dynamic weighted load balancing weight and high and low number of HTTP proxy sessions.	user	Not Specified							
hw-session-hold-time *	Time to hold sessions before purging on secondary node.	integer	Minimum value: 0 Maximum value: 180	10						
hw-session-sync-delay *	Time to wait before session sync starts on primary node.	integer	Minimum value: 0 Maximum value: 3600	150						
hw-session-sync-dev *	Hardware session sync interface.	string	Maximum length: 15							
imap-proxy-threshold	Dynamic weighted load balancing weight and high and low number of IMAP proxy sessions.	user	Not Specified							
key	Key.	password	Not Specified							
l2ep-eth-type	Telnet session HA heartbeat packet Ethertype (4-digit hex).	string	Maximum length: 4	8893						
link-failed-signal	Enable to shut down all interfaces for 1 sec after a failover. Use if gratuitous ARPs do not update network.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>				Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									

Parameter	Description	Type	Size	Default						
load-balance-all	Enable to load balance TCP sessions. Disable to load balance proxy sessions only.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable load balance.</td></tr><tr><td><i>disable</i></td><td>Disable load balance.</td></tr></table>	Option	Description	<i>enable</i>	Enable load balance.	<i>disable</i>	Disable load balance.			
	Option	Description								
	<i>enable</i>	Enable load balance.								
<i>disable</i>	Disable load balance.									
logical-sn	Enable/disable usage of the logical serial number.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable usage of the logical serial number.</td></tr><tr><td><i>disable</i></td><td>Disable usage of the logical serial number.</td></tr></table>	Option	Description	<i>enable</i>	Enable usage of the logical serial number.	<i>disable</i>	Disable usage of the logical serial number.			
	Option	Description								
	<i>enable</i>	Enable usage of the logical serial number.								
<i>disable</i>	Disable usage of the logical serial number.									
memory-based-failover	Enable/disable memory based failover.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
	Option	Description								
	<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.									
memory-compatible-mode	Enable/disable memory compatible mode.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
	Option	Description								
	<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.									
memory-failover-flip-timeout	Time to wait between subsequent memory based failovers in minutes.	integer	Minimum value: 6 Maximum value: 2147483647	6						
memory-failover-monitor-period	Duration of high memory usage before memory based failover is triggered in seconds.	integer	Minimum value: 1 Maximum value: 300	60						
memory-failover-sample-rate	Rate at which memory usage is sampled in order to measure memory usage in seconds.	integer	Minimum value: 1 Maximum value: 60	1						

Parameter	Description	Type	Size	Default								
memory-failover-threshold	Memory usage threshold to trigger memory based failover (0 means using conserve mode threshold in system.global).	integer	Minimum value: 0 Maximum value: 95	0								
memory-threshold	Dynamic weighted load balancing memory usage weight and high and low thresholds.	user	Not Specified									
mode	HA mode. Must be the same for all members. FGSP requires standalone.	option	-	standalone								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>standalone</i></td><td>Standalone mode.</td></tr><tr><td><i>a-a</i></td><td>Active-active mode.</td></tr><tr><td><i>a-p</i></td><td>Active-passive mode.</td></tr></table>				Option	Description	<i>standalone</i>	Standalone mode.	<i>a-a</i>	Active-active mode.	<i>a-p</i>	Active-passive mode.
Option	Description											
<i>standalone</i>	Standalone mode.											
<i>a-a</i>	Active-active mode.											
<i>a-p</i>	Active-passive mode.											
monitor	Interfaces to check for port monitoring (or link failure).	user	Not Specified									
multicast-ttl	HA multicast TTL on primary.	integer	Minimum value: 5 Maximum value: 3600	600								
nntp-proxy-threshold	Dynamic weighted load balancing weight and high and low number of NNTP proxy sessions.	user	Not Specified									
override	Enable and increase the priority of the unit that should always be primary.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>				Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
override-wait-time	Delay negotiating if override is enabled. Reduces how often the cluster negotiates.	integer	Minimum value: 0 Maximum value: 3600	0								
password	Cluster password. Must be the same for all members.	password	Not Specified									
pingserver-failover-threshold	Remote IP monitoring failover threshold.	integer	Minimum value: 0 Maximum value: 50	0								

Parameter	Description	Type	Size	Default						
pingserver-flip-timeout	Time to wait in minutes before renegotiating after a remote IP monitoring failover.	integer	Minimum value: 6 Maximum value: 2147483647	60						
pingserver-monitor-interface	Interfaces to check for remote IP monitoring.	user	Not Specified							
pingserver-secondary-force-reset	Enable to force the cluster to negotiate after a remote IP monitoring failover.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable force reset of secondary after PING server failure.</td></tr><tr><td><i>disable</i></td><td>Disable force reset of secondary after PING server failure.</td></tr></table>				Option	Description	<i>enable</i>	Enable force reset of secondary after PING server failure.	<i>disable</i>	Disable force reset of secondary after PING server failure.
Option	Description									
<i>enable</i>	Enable force reset of secondary after PING server failure.									
<i>disable</i>	Disable force reset of secondary after PING server failure.									
pop3-proxy-threshold	Dynamic weighted load balancing weight and high and low number of POP3 proxy sessions.	user	Not Specified							
priority	Increase the priority to select the primary unit.	integer	Minimum value: 0 Maximum value: 255	128						
route-hold	Time to wait between routing table updates to the cluster.	integer	Minimum value: 0 Maximum value: 3600	10						
route-ttl	TTL for primary unit routes. Increase to maintain active routes during failover.	integer	Minimum value: 5 Maximum value: 3600	10						
route-wait	Time to wait before sending new routes to the cluster.	integer	Minimum value: 0 Maximum value: 3600	0						
schedule	Type of A-A load balancing. Use none if you have external load balancers.	option	-	round-robin						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>None.</td></tr><tr><td><i>hub</i></td><td>Hub.</td></tr></table>				Option	Description	<i>none</i>	None.	<i>hub</i>	Hub.
Option	Description									
<i>none</i>	None.									
<i>hub</i>	Hub.									



Parameter	Description	Type	Size	Default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>leastconnection</i></td><td>Least connection.</td></tr><tr><td><i>round-robin</i></td><td>Round robin.</td></tr><tr><td><i>weight-round-robin</i></td><td>Weight round robin.</td></tr><tr><td><i>random</i></td><td>Random.</td></tr><tr><td><i>ip</i></td><td>IP.</td></tr><tr><td><i>ipport</i></td><td>IP port.</td></tr></table>	Option	Description	<i>leastconnection</i>	Least connection.	<i>round-robin</i>	Round robin.	<i>weight-round-robin</i>	Weight round robin.	<i>random</i>	Random.	<i>ip</i>	IP.	<i>ipport</i>	IP port.			
	Option	Description																
	<i>leastconnection</i>	Least connection.																
	<i>round-robin</i>	Round robin.																
	<i>weight-round-robin</i>	Weight round robin.																
	<i>random</i>	Random.																
	<i>ip</i>	IP.																
<i>ipport</i>	IP port.																	
session-pickup	Enable/disable session pickup. Enabling it can reduce session down time when fail over happens.	option	-	disable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable session pickup.</td></tr><tr><td><i>disable</i></td><td>Disable session pickup.</td></tr></table>	Option	Description	<i>enable</i>	Enable session pickup.	<i>disable</i>	Disable session pickup.											
	Option	Description																
	<i>enable</i>	Enable session pickup.																
<i>disable</i>	Disable session pickup.																	
session-pickup-connectionless	Enable/disable UDP and ICMP session sync.	option	-	disable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.											
	Option	Description																
	<i>enable</i>	Enable setting.																
<i>disable</i>	Disable setting.																	
session-pickup-delay	Enable to sync sessions longer than 30 sec. Only longer lived sessions need to be synced.	option	-	disable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.											
	Option	Description																
	<i>enable</i>	Enable setting.																
<i>disable</i>	Disable setting.																	
session-pickup-expectation	Enable/disable session helper expectation session sync for FGSP.	option	-	disable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.											
	Option	Description																
	<i>enable</i>	Enable setting.																
<i>disable</i>	Disable setting.																	
session-pickup-nat	Enable/disable NAT session sync for FGSP.	option	-	disable														

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
session-sync-dev	Offload session-sync process to kernel and sync sessions using connected interface(s) directly.	user	Not Specified	
smtp-proxy-threshold	Dynamic weighted load balancing weight and high and low number of SMTP proxy sessions.	user	Not Specified	
ssd-failover *	Enable/disable automatic HA failover on SSD disk failure.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
standalone-config-sync	Enable/disable FGSP configuration synchronization.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
standalone-mgmt-vdom	Enable/disable standalone management VDOM.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
sync-config	Enable/disable configuration synchronization.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable configuration synchronization.		
	<i>disable</i>	Disable configuration synchronization.		
sync-packet-balance	Enable/disable HA packet distribution to multiple CPUs.	option	-	disable

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable HA packet distribution to multiple CPUs.		
	<i>disable</i>	Disable HA packet distribution to multiple CPUs.		
unicast-gateway *	Default route gateway for unicast interface.	ipv4-address	Not Specified	0.0.0.0
unicast-hb *	Enable/disable unicast heartbeat.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
unicast-hb-netmask *	Unicast heartbeat netmask.	ipv4-netmask	Not Specified	0.0.0.0
unicast-hb-peerip *	Unicast heartbeat peer IP.	ipv4-address	Not Specified	0.0.0.0
unicast-status *	Enable/disable unicast connection.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
uninterruptible-primary-wait	Number of minutes the primary HA unit waits before the secondary HA unit is considered upgraded and the system is started before starting its own upgrade.	integer	Minimum value: 15 Maximum value: 300	30
uninterruptible-upgrade	Enable to upgrade a cluster without blocking network traffic.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
vcluster-id	Cluster ID.	integer	Minimum value: 0 Maximum value: 255	0
vcluster2	Enable/disable virtual cluster 2 for virtual clustering.	option	-	disable

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
vdom	VDOMs in virtual cluster 1.	user	Not Specified	
weight	Weighted round robin weight for each cluster unit. Syntax <priority> <weight>.	user	Not Specified	0 40

\* This parameter may not exist in some models.

\*\* Values may differ between models.

### config ha-mgmt-interfaces

Parameter	Description	Type	Size	Default
id	Table ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
interface	Interface to reserve for HA management.	string	Maximum length: 15	
dst	Default route destination for reserved HA management interface.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0
gateway	Default route gateway for reserved HA management interface.	ipv4-address	Not Specified	0.0.0.0
gateway6	Default IPv6 gateway for reserved HA management interface.	ipv6-address	Not Specified	::

### config secondary-vcluster

Parameter	Description	Type	Size	Default
vcluster-id	Cluster ID.	integer	Minimum value: 0 Maximum value: 255	1
override	Enable and increase the priority of the unit that should always be primary.	option	-	enable

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
priority	Increase the priority to select the primary unit.	integer	Minimum value: 0 Maximum value: 255	128
override-wait-time	Delay negotiating if override is enabled. Reduces how often the cluster negotiates.	integer	Minimum value: 0 Maximum value: 3600	0
monitor	Interfaces to check for port monitoring (or link failure).	user	Not Specified	
pingserver-monitor-interface	Interfaces to check for remote IP monitoring.	user	Not Specified	
pingserver-failover-threshold	Remote IP monitoring failover threshold.	integer	Minimum value: 0 Maximum value: 50	0
pingserver-secondary-force-reset	Enable to force the cluster to negotiate after a remote IP monitoring failover.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable force reset of secondary after PING server failure.		
	<i>disable</i>	Disable force reset of secondary after PING server failure.		
vdom	VDOMs in virtual cluster 2.	user	Not Specified	

## config unicast-peers

Parameter	Description	Type	Size	Default
id	Table ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
peer-ip	Unicast peer IP.	ipv4-address	Not Specified	0.0.0.0

---

## config system ike

Configure IKE global attributes.

```
config system ike
  Description: Configure IKE global attributes.
  config dh-group-1
    Description: Diffie-Hellman group 1 (MODP-768).
    set mode [software|hardware|...]
    set keypair-cache [global|custom]
    set keypair-count {integer}
  end
  config dh-group-14
    Description: Diffie-Hellman group 14 (MODP-2048).
    set mode [software|hardware|...]
    set keypair-cache [global|custom]
    set keypair-count {integer}
  end
  config dh-group-15
    Description: Diffie-Hellman group 15 (MODP-3072).
    set mode [software|hardware|...]
    set keypair-cache [global|custom]
    set keypair-count {integer}
  end
  config dh-group-16
    Description: Diffie-Hellman group 16 (MODP-4096).
    set mode [software|hardware|...]
    set keypair-cache [global|custom]
    set keypair-count {integer}
  end
  config dh-group-17
    Description: Diffie-Hellman group 17 (MODP-6144).
    set mode [software|hardware|...]
    set keypair-cache [global|custom]
    set keypair-count {integer}
  end
  config dh-group-18
    Description: Diffie-Hellman group 18 (MODP-8192).
    set mode [software|hardware|...]
    set keypair-cache [global|custom]
    set keypair-count {integer}
  end
  config dh-group-19
    Description: Diffie-Hellman group 19 (EC-P256).
    set mode [software|hardware|...]
    set keypair-cache [global|custom]
    set keypair-count {integer}
  end
  config dh-group-2
    Description: Diffie-Hellman group 2 (MODP-1024).
    set mode [software|hardware|...]
    set keypair-cache [global|custom]
    set keypair-count {integer}
  end
  config dh-group-20
    Description: Diffie-Hellman group 20 (EC-P384).
```

```

        set mode [software|hardware|...]
        set keypair-cache [global|custom]
        set keypair-count {integer}
    end
    config dh-group-21
        Description: Diffie-Hellman group 21 (EC-P521).
        set mode [software|hardware|...]
        set keypair-cache [global|custom]
        set keypair-count {integer}
    end
    config dh-group-27
        Description: Diffie-Hellman group 27 (EC-P224BP).
        set mode [software|hardware|...]
        set keypair-cache [global|custom]
        set keypair-count {integer}
    end
    config dh-group-28
        Description: Diffie-Hellman group 28 (EC-P256BP).
        set mode [software|hardware|...]
        set keypair-cache [global|custom]
        set keypair-count {integer}
    end
    config dh-group-29
        Description: Diffie-Hellman group 29 (EC-P384BP).
        set mode [software|hardware|...]
        set keypair-cache [global|custom]
        set keypair-count {integer}
    end
    config dh-group-30
        Description: Diffie-Hellman group 30 (EC-P512BP).
        set mode [software|hardware|...]
        set keypair-cache [global|custom]
        set keypair-count {integer}
    end
    config dh-group-31
        Description: Diffie-Hellman group 31 (EC-X25519).
        set mode [software|hardware|...]
        set keypair-cache [global|custom]
        set keypair-count {integer}
    end
    config dh-group-32
        Description: Diffie-Hellman group 32 (EC-X448).
        set mode [software|hardware|...]
        set keypair-cache [global|custom]
        set keypair-count {integer}
    end
    config dh-group-5
        Description: Diffie-Hellman group 5 (MODP-1536).
        set mode [software|hardware|...]
        set keypair-cache [global|custom]
        set keypair-count {integer}
    end
    set dh-keypair-cache [enable|disable]
    set dh-keypair-count {integer}
    set dh-keypair-throttle [enable|disable]
    set dh-mode [software|hardware]

```

```

set dh-multiprocess [enable|disable]
set dh-worker-count {integer}
set embryonic-limit {integer}
end

```

## config system ike

Parameter	Description	Type	Size	Default						
dh-keypair-cache	Enable/disable Diffie-Hellman key pair cache.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Diffie-Hellman key pair cache.</td></tr><tr><td><i>disable</i></td><td>Disable Diffie-Hellman key pair cache.</td></tr></table>	Option	Description	<i>enable</i>	Enable Diffie-Hellman key pair cache.	<i>disable</i>	Disable Diffie-Hellman key pair cache.			
Option	Description									
<i>enable</i>	Enable Diffie-Hellman key pair cache.									
<i>disable</i>	Disable Diffie-Hellman key pair cache.									
dh-keypair-count	Number of key pairs to pre-generate for each Diffie-Hellman group (per-worker).	integer	Minimum value: 0 Maximum value: 50000	100 **						
dh-keypair-throttle	Enable/disable Diffie-Hellman key pair cache CPU throttling.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Diffie-Hellman key pair cache CPU throttling.</td></tr><tr><td><i>disable</i></td><td>Disable Diffie-Hellman key pair cache CPU throttling.</td></tr></table>	Option	Description	<i>enable</i>	Enable Diffie-Hellman key pair cache CPU throttling.	<i>disable</i>	Disable Diffie-Hellman key pair cache CPU throttling.			
Option	Description									
<i>enable</i>	Enable Diffie-Hellman key pair cache CPU throttling.									
<i>disable</i>	Disable Diffie-Hellman key pair cache CPU throttling.									
dh-mode	Use software (CPU) or hardware (CPX) to perform Diffie-Hellman calculations.	option	-	hardware **						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>software</i></td><td>Prefer CPU to perform Diffie-Hellman calculations.</td></tr><tr><td><i>hardware</i></td><td>Prefer CPX to perform Diffie-Hellman calculations.</td></tr></table>	Option	Description	<i>software</i>	Prefer CPU to perform Diffie-Hellman calculations.	<i>hardware</i>	Prefer CPX to perform Diffie-Hellman calculations.			
Option	Description									
<i>software</i>	Prefer CPU to perform Diffie-Hellman calculations.									
<i>hardware</i>	Prefer CPX to perform Diffie-Hellman calculations.									
dh-multiprocess	Enable/disable multiprocess Diffie-Hellman daemon for IKE.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable multiprocess Diffie-Hellman for IKE.</td></tr><tr><td><i>disable</i></td><td>Disable multiprocess Diffie-Hellman for IKE.</td></tr></table>	Option	Description	<i>enable</i>	Enable multiprocess Diffie-Hellman for IKE.	<i>disable</i>	Disable multiprocess Diffie-Hellman for IKE.			
Option	Description									
<i>enable</i>	Enable multiprocess Diffie-Hellman for IKE.									
<i>disable</i>	Disable multiprocess Diffie-Hellman for IKE.									



Parameter	Description	Type	Size	Default
dh-worker-count	Number of Diffie-Hellman workers to start.	integer	Minimum value: 1 Maximum value: 8 **	0
embryonic-limit	Maximum number of IPsec tunnels to negotiate simultaneously.	integer	Minimum value: 50 Maximum value: 20000	5000 **

\*\* Values may differ between models.

### config dh-group-1

Parameter	Description	Type	Size	Default
mode	Use software (CPU) or hardware (CPX) to perform calculations for this Diffie-Hellman group.	option	-	global
	<b>Option</b>	<b>Description</b>		
	<i>software</i>	Prefer CPU to perform Diffie-Hellman calculations.		
	<i>hardware</i>	Prefer CPX to perform Diffie-Hellman calculations.		
	<i>global</i>	Use global dh-mode setting.		
keypair-cache	Configure custom key pair cache size for this Diffie-Hellman group.	option	-	global
	<b>Option</b>	<b>Description</b>		
	<i>global</i>	Use global Diffie-Hellman key pair cache setting.		
	<i>custom</i>	Use custom Diffie-Hellman key pair cache setting.		
keypair-count	Number of key pairs to pre-generate for this Diffie-Hellman group (per-worker).	integer	Minimum value: 0 Maximum value: 50000	0

### config dh-group-14

Parameter	Description	Type	Size	Default
mode	Use software (CPU) or hardware (CPX) to perform calculations for this Diffie-Hellman group.	option	-	global

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>software</i>	Prefer CPU to perform Diffie-Hellman calculations.		
	<i>hardware</i>	Prefer CPX to perform Diffie-Hellman calculations.		
	<i>global</i>	Use global dh-mode setting.		
keypair-cache	Configure custom key pair cache size for this Diffie-Hellman group.	option	-	global
	<b>Option</b>	<b>Description</b>		
	<i>global</i>	Use global Diffie-Hellman key pair cache setting.		
	<i>custom</i>	Use custom Diffie-Hellman key pair cache setting.		
keypair-count	Number of key pairs to pre-generate for this Diffie-Hellman group (per-worker).	integer	Minimum value: 0 Maximum value: 50000	0

### config dh-group-15

Parameter	Description	Type	Size	Default
mode	Use software (CPU) or hardware (CPX) to perform calculations for this Diffie-Hellman group.	option	-	global
	<b>Option</b>	<b>Description</b>		
	<i>software</i>	Prefer CPU to perform Diffie-Hellman calculations.		
	<i>hardware</i>	Prefer CPX to perform Diffie-Hellman calculations.		
	<i>global</i>	Use global dh-mode setting.		
keypair-cache	Configure custom key pair cache size for this Diffie-Hellman group.	option	-	global
	<b>Option</b>	<b>Description</b>		
	<i>global</i>	Use global Diffie-Hellman key pair cache setting.		
	<i>custom</i>	Use custom Diffie-Hellman key pair cache setting.		
keypair-count	Number of key pairs to pre-generate for this Diffie-Hellman group (per-worker).	integer	Minimum value: 0 Maximum value: 50000	0

## config dh-group-16

Parameter	Description	Type	Size	Default
mode	Use software (CPU) or hardware (CPX) to perform calculations for this Diffie-Hellman group.	option	-	global
	<b>Option</b>	<b>Description</b>		
	<i>software</i>	Prefer CPU to perform Diffie-Hellman calculations.		
	<i>hardware</i>	Prefer CPX to perform Diffie-Hellman calculations.		
	<i>global</i>	Use global dh-mode setting.		
keypair-cache	Configure custom key pair cache size for this Diffie-Hellman group.	option	-	global
	<b>Option</b>	<b>Description</b>		
	<i>global</i>	Use global Diffie-Hellman key pair cache setting.		
	<i>custom</i>	Use custom Diffie-Hellman key pair cache setting.		
keypair-count	Number of key pairs to pre-generate for this Diffie-Hellman group (per-worker).	integer	Minimum value: 0 Maximum value: 50000	0

## config dh-group-17

Parameter	Description	Type	Size	Default
mode	Use software (CPU) or hardware (CPX) to perform calculations for this Diffie-Hellman group.	option	-	global
	<b>Option</b>	<b>Description</b>		
	<i>software</i>	Prefer CPU to perform Diffie-Hellman calculations.		
	<i>hardware</i>	Prefer CPX to perform Diffie-Hellman calculations.		
	<i>global</i>	Use global dh-mode setting.		
keypair-cache	Configure custom key pair cache size for this Diffie-Hellman group.	option	-	global
	<b>Option</b>	<b>Description</b>		
	<i>global</i>	Use global Diffie-Hellman key pair cache setting.		
	<i>custom</i>	Use custom Diffie-Hellman key pair cache setting.		

Parameter	Description	Type	Size	Default
keypair-count	Number of key pairs to pre-generate for this Diffie-Hellman group (per-worker).	integer	Minimum value: 0 Maximum value: 50000	0

### config dh-group-18

Parameter	Description	Type	Size	Default
mode	Use software (CPU) or hardware (CPX) to perform calculations for this Diffie-Hellman group.	option	-	global
	<b>Option</b>	<b>Description</b>		
	<i>software</i>	Prefer CPU to perform Diffie-Hellman calculations.		
	<i>hardware</i>	Prefer CPX to perform Diffie-Hellman calculations.		
	<i>global</i>	Use global dh-mode setting.		
keypair-cache	Configure custom key pair cache size for this Diffie-Hellman group.	option	-	global
	<b>Option</b>	<b>Description</b>		
	<i>global</i>	Use global Diffie-Hellman key pair cache setting.		
	<i>custom</i>	Use custom Diffie-Hellman key pair cache setting.		
keypair-count	Number of key pairs to pre-generate for this Diffie-Hellman group (per-worker).	integer	Minimum value: 0 Maximum value: 50000	0

### config dh-group-19

Parameter	Description	Type	Size	Default
mode	Use software (CPU) or hardware (CPX) to perform calculations for this Diffie-Hellman group.	option	-	global
	<b>Option</b>	<b>Description</b>		
	<i>software</i>	Prefer CPU to perform Diffie-Hellman calculations.		
	<i>hardware</i>	Prefer CPX to perform Diffie-Hellman calculations.		
	<i>global</i>	Use global dh-mode setting.		

Parameter	Description	Type	Size	Default
keypair-cache	Configure custom key pair cache size for this Diffie-Hellman group.	option	-	global
	<b>Option</b>	<b>Description</b>		
	<i>global</i>	Use global Diffie-Hellman key pair cache setting.		
	<i>custom</i>	Use custom Diffie-Hellman key pair cache setting.		
keypair-count	Number of key pairs to pre-generate for this Diffie-Hellman group (per-worker).	integer	Minimum value: 0 Maximum value: 50000	0

### config dh-group-2

Parameter	Description	Type	Size	Default
mode	Use software (CPU) or hardware (CPX) to perform calculations for this Diffie-Hellman group.	option	-	global
	<b>Option</b>	<b>Description</b>		
	<i>software</i>	Prefer CPU to perform Diffie-Hellman calculations.		
	<i>hardware</i>	Prefer CPX to perform Diffie-Hellman calculations.		
	<i>global</i>	Use global dh-mode setting.		
keypair-cache	Configure custom key pair cache size for this Diffie-Hellman group.	option	-	global
	<b>Option</b>	<b>Description</b>		
	<i>global</i>	Use global Diffie-Hellman key pair cache setting.		
	<i>custom</i>	Use custom Diffie-Hellman key pair cache setting.		
keypair-count	Number of key pairs to pre-generate for this Diffie-Hellman group (per-worker).	integer	Minimum value: 0 Maximum value: 50000	0

## config dh-group-20

Parameter	Description	Type	Size	Default
mode	Use software (CPU) or hardware (CPX) to perform calculations for this Diffie-Hellman group.	option	-	global
	<b>Option</b>	<b>Description</b>		
	<i>software</i>	Prefer CPU to perform Diffie-Hellman calculations.		
	<i>hardware</i>	Prefer CPX to perform Diffie-Hellman calculations.		
	<i>global</i>	Use global dh-mode setting.		
keypair-cache	Configure custom key pair cache size for this Diffie-Hellman group.	option	-	global
	<b>Option</b>	<b>Description</b>		
	<i>global</i>	Use global Diffie-Hellman key pair cache setting.		
	<i>custom</i>	Use custom Diffie-Hellman key pair cache setting.		
keypair-count	Number of key pairs to pre-generate for this Diffie-Hellman group (per-worker).	integer	Minimum value: 0 Maximum value: 50000	0

## config dh-group-21

Parameter	Description	Type	Size	Default
mode	Use software (CPU) or hardware (CPX) to perform calculations for this Diffie-Hellman group.	option	-	global
	<b>Option</b>	<b>Description</b>		
	<i>software</i>	Prefer CPU to perform Diffie-Hellman calculations.		
	<i>hardware</i>	Prefer CPX to perform Diffie-Hellman calculations.		
	<i>global</i>	Use global dh-mode setting.		
keypair-cache	Configure custom key pair cache size for this Diffie-Hellman group.	option	-	global
	<b>Option</b>	<b>Description</b>		
	<i>global</i>	Use global Diffie-Hellman key pair cache setting.		
	<i>custom</i>	Use custom Diffie-Hellman key pair cache setting.		

Parameter	Description	Type	Size	Default
keypair-count	Number of key pairs to pre-generate for this Diffie-Hellman group (per-worker).	integer	Minimum value: 0 Maximum value: 50000	0

### config dh-group-27

Parameter	Description	Type	Size	Default
mode	Use software (CPU) or hardware (CPX) to perform calculations for this Diffie-Hellman group.	option	-	global
	<b>Option</b>	<b>Description</b>		
	<i>software</i>	Prefer CPU to perform Diffie-Hellman calculations.		
	<i>hardware</i>	Prefer CPX to perform Diffie-Hellman calculations.		
	<i>global</i>	Use global dh-mode setting.		
keypair-cache	Configure custom key pair cache size for this Diffie-Hellman group.	option	-	global
	<b>Option</b>	<b>Description</b>		
	<i>global</i>	Use global Diffie-Hellman key pair cache setting.		
	<i>custom</i>	Use custom Diffie-Hellman key pair cache setting.		
keypair-count	Number of key pairs to pre-generate for this Diffie-Hellman group (per-worker).	integer	Minimum value: 0 Maximum value: 50000	0

### config dh-group-28

Parameter	Description	Type	Size	Default
mode	Use software (CPU) or hardware (CPX) to perform calculations for this Diffie-Hellman group.	option	-	global
	<b>Option</b>	<b>Description</b>		
	<i>software</i>	Prefer CPU to perform Diffie-Hellman calculations.		
	<i>hardware</i>	Prefer CPX to perform Diffie-Hellman calculations.		
	<i>global</i>	Use global dh-mode setting.		

Parameter	Description	Type	Size	Default
keypair-cache	Configure custom key pair cache size for this Diffie-Hellman group.	option	-	global
	<b>Option</b>	<b>Description</b>		
	<i>global</i>	Use global Diffie-Hellman key pair cache setting.		
	<i>custom</i>	Use custom Diffie-Hellman key pair cache setting.		
keypair-count	Number of key pairs to pre-generate for this Diffie-Hellman group (per-worker).	integer	Minimum value: 0 Maximum value: 50000	0

### config dh-group-29

Parameter	Description	Type	Size	Default
mode	Use software (CPU) or hardware (CPX) to perform calculations for this Diffie-Hellman group.	option	-	global
	<b>Option</b>	<b>Description</b>		
	<i>software</i>	Prefer CPU to perform Diffie-Hellman calculations.		
	<i>hardware</i>	Prefer CPX to perform Diffie-Hellman calculations.		
	<i>global</i>	Use global dh-mode setting.		
keypair-cache	Configure custom key pair cache size for this Diffie-Hellman group.	option	-	global
	<b>Option</b>	<b>Description</b>		
	<i>global</i>	Use global Diffie-Hellman key pair cache setting.		
	<i>custom</i>	Use custom Diffie-Hellman key pair cache setting.		
keypair-count	Number of key pairs to pre-generate for this Diffie-Hellman group (per-worker).	integer	Minimum value: 0 Maximum value: 50000	0



## config dh-group-30

Parameter	Description	Type	Size	Default
mode	Use software (CPU) or hardware (CPX) to perform calculations for this Diffie-Hellman group.	option	-	global
	<b>Option</b>	<b>Description</b>		
	<i>software</i>	Prefer CPU to perform Diffie-Hellman calculations.		
	<i>hardware</i>	Prefer CPX to perform Diffie-Hellman calculations.		
	<i>global</i>	Use global dh-mode setting.		
keypair-cache	Configure custom key pair cache size for this Diffie-Hellman group.	option	-	global
	<b>Option</b>	<b>Description</b>		
	<i>global</i>	Use global Diffie-Hellman key pair cache setting.		
	<i>custom</i>	Use custom Diffie-Hellman key pair cache setting.		
keypair-count	Number of key pairs to pre-generate for this Diffie-Hellman group (per-worker).	integer	Minimum value: 0 Maximum value: 50000	0

## config dh-group-31

Parameter	Description	Type	Size	Default
mode	Use software (CPU) or hardware (CPX) to perform calculations for this Diffie-Hellman group.	option	-	global
	<b>Option</b>	<b>Description</b>		
	<i>software</i>	Prefer CPU to perform Diffie-Hellman calculations.		
	<i>hardware</i>	Prefer CPX to perform Diffie-Hellman calculations.		
	<i>global</i>	Use global dh-mode setting.		
keypair-cache	Configure custom key pair cache size for this Diffie-Hellman group.	option	-	global
	<b>Option</b>	<b>Description</b>		
	<i>global</i>	Use global Diffie-Hellman key pair cache setting.		
	<i>custom</i>	Use custom Diffie-Hellman key pair cache setting.		

Parameter	Description	Type	Size	Default
keypair-count	Number of key pairs to pre-generate for this Diffie-Hellman group (per-worker).	integer	Minimum value: 0 Maximum value: 50000	0

### config dh-group-32

Parameter	Description	Type	Size	Default
mode	Use software (CPU) or hardware (CPX) to perform calculations for this Diffie-Hellman group.	option	-	global
	<b>Option</b>	<b>Description</b>		
	<i>software</i>	Prefer CPU to perform Diffie-Hellman calculations.		
	<i>hardware</i>	Prefer CPX to perform Diffie-Hellman calculations.		
	<i>global</i>	Use global dh-mode setting.		
keypair-cache	Configure custom key pair cache size for this Diffie-Hellman group.	option	-	global
	<b>Option</b>	<b>Description</b>		
	<i>global</i>	Use global Diffie-Hellman key pair cache setting.		
	<i>custom</i>	Use custom Diffie-Hellman key pair cache setting.		
keypair-count	Number of key pairs to pre-generate for this Diffie-Hellman group (per-worker).	integer	Minimum value: 0 Maximum value: 50000	0

### config dh-group-5

Parameter	Description	Type	Size	Default
mode	Use software (CPU) or hardware (CPX) to perform calculations for this Diffie-Hellman group.	option	-	global
	<b>Option</b>	<b>Description</b>		
	<i>software</i>	Prefer CPU to perform Diffie-Hellman calculations.		
	<i>hardware</i>	Prefer CPX to perform Diffie-Hellman calculations.		
	<i>global</i>	Use global dh-mode setting.		

Parameter	Description	Type	Size	Default
keypair-cache	Configure custom key pair cache size for this Diffie-Hellman group.	option	-	global
	Option	Description		
	<i>global</i>	Use global Diffie-Hellman key pair cache setting.		
	<i>custom</i>	Use custom Diffie-Hellman key pair cache setting.		
keypair-count	Number of key pairs to pre-generate for this Diffie-Hellman group (per-worker).	integer	Minimum value: 0 Maximum value: 50000	0

## config system interface

Configure interfaces.

```
config system interface
    Description: Configure interfaces.
    edit <name>
        set ac-name {string}
        set aggregate {string}
        set algorithm [L2|L3|...]
        set alias {string}
        set allowaccess {option1}, {option2}, ...
        set ap-discover [enable|disable]
        set arpforward [enable|disable]
        set atm-protocol [none|ipoa]
        set auth-cert {string}
        set auth-portal-addr {string}
        set auth-type [auto|pap|...]
        set auto-auth-extension-device [enable|disable]
        set bandwidth-measure-time {integer}
        set bfd [global|enable|...]
        set bfd-desired-min-tx {integer}
        set bfd-detect-mult {integer}
        set bfd-required-min-rx {integer}
        set broadcast-forward [enable|disable]
        set cli-conn-status {integer}
        config client-options
            Description: DHCP client options.
            edit <id>
                set code {integer}
                set type [hex|string|...]
                set value {string}
                set ip {user}
            next
        end
        set color {integer}
        set dedicated-to [none|management]
```

```

set defaultgw [enable|disable]
set description {var-string}
set detected-peer-mtu {integer}
set detectprotocol {option1}, {option2}, ...
set detectserver {user}
set device-identification [enable|disable]
set device-user-identification [enable|disable]
set devindex {integer}
set dhcp-classless-route-addition [enable|disable]
set dhcp-client-identifier {string}
set dhcp-relay-agent-option [enable|disable]
set dhcp-relay-interface {string}
set dhcp-relay-interface-select-method [auto|sdwan|...]
set dhcp-relay-ip {user}
set dhcp-relay-link-selection {ipv4-address}
set dhcp-relay-request-all-server [disable|enable]
set dhcp-relay-service [disable|enable]
set dhcp-relay-type [regular|ipsec]
set dhcp-renew-time {integer}
config dhcp-snooping-server-list
    Description: Configure DHCP server access list.
    edit <name>
        set server-ip {ipv4-address}
    next
end
set disc-retry-timeout {integer}
set disconnect-threshold {integer}
set distance {integer}
set dns-server-override [enable|disable]
set dns-server-protocol {option1}, {option2}, ...
set drop-fragment [enable|disable]
set drop-overlapped-fragment [enable|disable]
set egress-cos [disable|cos0|...]
config egress-queues
    Description: Configure queues of NP port on egress path.
    set cos0 {string}
    set cos1 {string}
    set cos2 {string}
    set cos3 {string}
    set cos4 {string}
    set cos5 {string}
    set cos6 {string}
    set cos7 {string}
end
set egress-shaping-profile {string}
set estimated-downstream-bandwidth {integer}
set estimated-upstream-bandwidth {integer}
set explicit-ftp-proxy [enable|disable]
set explicit-web-proxy [enable|disable]
set external [enable|disable]
set fail-action-on-extender [soft-restart|hard-restart|...]
set fail-alert-interfaces <name1>, <name2>, ...
set fail-alert-method [link-failed-signal|link-down]
set fail-detect [enable|disable]
set fail-detect-option {option1}, {option2}, ...
set fortilink [enable|disable]

```

```

set fortilink-backup-link {integer}
set fortilink-neighbor-detect [lldp|fortilink]
set fortilink-split-interface [enable|disable]
set forward-domain {integer}
set forward-error-correction [none|disable|...]
set gateway-address {ipv4-address}
set gi-gk [enable|disable]
set gwaddr {ipv4-address}
set gwdetect [enable|disable]
set ha-priority {integer}
set icmp-accept-redirect [enable|disable]
set icmp-send-redirect [enable|disable]
set ident-accept [enable|disable]
set idle-timeout {integer}
set inbandwidth {integer}
set ingress-cos [disable|cos0|...]
set ingress-shaping-profile {string}
set ingress-spillover-threshold {integer}
set interface {string}
set internal {integer}
set ip {ipv4-classnet-host}
set ip-managed-by-fortiipam [enable|disable]
set ipmac [enable|disable]
set ips-sniffer-mode [enable|disable]
set ipunnumbered {ipv4-address}
config ipv6
    Description: IPv6 of interface.
    set ip6-mode [static|dhcp|...]
    set nd-mode [basic|SEND-compatible]
    set nd-cert {string}
    set nd-security-level {integer}
    set nd-timestamp-delta {integer}
    set nd-timestamp-fuzz {integer}
    set nd-cga-modifier {user}
    set ip6-dns-server-override [enable|disable]
    set ip6-address {ipv6-prefix}
    config ip6-extra-addr
        Description: Extra IPv6 address prefixes of interface.
        edit <prefix>
        next
    end
    set ip6-allowaccess {option1}, {option2}, ...
    set ip6-send-adv [enable|disable]
    set icmp6-send-redirect [enable|disable]
    set ip6-manage-flag [enable|disable]
    set ip6-other-flag [enable|disable]
    set ip6-max-interval {integer}
    set ip6-min-interval {integer}
    set ip6-link-mtu {integer}
    set ra-send-mtu [enable|disable]
    set ip6-reachable-time {integer}
    set ip6-retrans-time {integer}
    set ip6-default-life {integer}
    set ip6-hop-limit {integer}
    set autoconf [enable|disable]
    set unique-autoconf-addr [enable|disable]

```

```

set interface-identifier {ipv6-address}
set ip6-prefix-mode [dhcp6|ra]
set ip6-upstream-interface {string}
set ip6-delegated-prefix-iaid {integer}
set ip6-subnet {ipv6-prefix}
config ip6-prefix-list
    Description: Advertised prefix list.
    edit <prefix>
        set autonomous-flag [enable|disable]
        set onlink-flag [enable|disable]
        set valid-life-time {integer}
        set preferred-life-time {integer}
        set rdns {user}
        set dnssl <domain1>, <domain2>, ...
    next
end
config ip6-delegated-prefix-list
    Description: Advertised IPv6 delegated prefix list.
    edit <prefix-id>
        set upstream-interface {string}
        set delegated-prefix-iaid {integer}
        set autonomous-flag [enable|disable]
        set onlink-flag [enable|disable]
        set subnet {ipv6-network}
        set rdns-service [delegated|default|...]
        set rdns {user}
    next
end
set dhcp6-relay-service [disable|enable]
set dhcp6-relay-type {option}
set dhcp6-relay-ip {user}
set dhcp6-client-options {option1}, {option2}, ...
set dhcp6-prefix-delegation [enable|disable]
set dhcp6-information-request [enable|disable]
config dhcp6-iapd-list
    Description: DHCPv6 IA-PD list.
    edit <iaid>
        set prefix-hint {ipv6-network}
        set prefix-hint-plt {integer}
        set prefix-hint-vlt {integer}
    next
end
set cli-conn6-status {integer}
set vrrp-virtual-mac6 [enable|disable]
set vrip6_link_local {ipv6-address}
config vrrp6
    Description: IPv6 VRRP configuration.
    edit <vrid>
        set vrgrp {integer}
        set vrip6 {ipv6-address}
        set priority {integer}
        set adv-interval {integer}
        set start-time {integer}
        set preempt [enable|disable]
        set accept-mode [enable|disable]
        set vrdst6 {ipv6-address}

```

```

        set status [enable|disable]
    next
end
end
set l2forward [enable|disable]
set l2tp-client [enable|disable]
config l2tp-client-settings
    Description: L2TP client settings.
    set user {string}
    set password {password}
    set peer-host {string}
    set peer-mask {ipv4-netmask}
    set peer-port {integer}
    set auth-type [auto|pap|...]
    set mtu {integer}
    set distance {integer}
    set priority {integer}
    set defaultgw [enable|disable]
    set ip {ipv4-classnet-host}
    set hello-interval {integer}
end
set lacp-ha-slave [enable|disable]
set lacp-mode [static|passive|...]
set lacp-speed [slow|fast]
set lcp-echo-interval {integer}
set lcp-max-echo-fails {integer}
set link-up-delay {integer}
set lldp-network-policy {string}
set lldp-reception [enable|disable|...]
set lldp-transmission [enable|disable|...]
set macaddr {mac-address}
set managed-subnetwork-size [32|64|...]
set management-ip {ipv4-classnet-host}
set measured-downstream-bandwidth {integer}
set measured-upstream-bandwidth {integer}
set mediatype [serdes-sfp|sgmii-sfp|...]
set member <interface-name1>, <interface-name2>, ...
set min-links {integer}
set min-links-down [operational|administrative]
set mode [static|dhcp|...]
set monitor-bandwidth [enable|disable]
set mtu {integer}
set mtu-override [enable|disable]
set mux-type [llc-encaps|vc-encaps]
set ndiscforward [enable|disable]
set netbios-forward [disable|enable]
set netflow-sampler [disable|tx|...]
set np-qos-profile {integer}
set outbandwidth {integer}
set padt-retry-timeout {integer}
set password {password}
set phy-mode {option}
set ping-serv-status {integer}
set poe [enable|disable]
set polling-interval {integer}
set pppoe-unnumbered-negotiate [enable|disable]

```

```

set pptp-auth-type [auto|pap|...]
set pptp-client [enable|disable]
set pptp-password {password}
set pptp-server-ip {ipv4-address}
set pptp-timeout {integer}
set pptp-user {string}
set preserve-session-route [enable|disable]
set priority {integer}
set priority-override [enable|disable]
set proxy-captive-portal [enable|disable]
set pvc-atm-qos [cbr|rt-vbr|...]
set pvc-chan {integer}
set pvc-crc {integer}
set pvc-pcr {integer}
set pvc-scr {integer}
set pvc-vlan-id {integer}
set pvc-vlan-rx-id {integer}
set pvc-vlan-rx-op [pass-through|replace|...]
set pvc-vlan-tx-id {integer}
set pvc-vlan-tx-op [pass-through|replace|...]
set reachable-time {integer}
set redundant-interface {string}
set remote-ip {ipv4-classnet-host}
set replacemsg-override-group {string}
set retransmission [disable|enable]
set ring-rx {integer}
set ring-tx {integer}
set role [lan|wan|...]
set sample-direction [tx|rx|...]
set sample-rate {integer}
set secondary-IP [enable|disable]
config secondaryip
    Description: Second IP address of interface.
    edit <id>
        set ip {ipv4-classnet-host}
        set allowaccess {option1}, {option2}, ...
        set gwdetect [enable|disable]
        set ping-serv-status {integer}
        set detectserver {user}
        set detectprotocol {option1}, {option2}, ...
        set ha-priority {integer}
    next
end
set security-8021x-dynamic-vlan-id {integer}
set security-8021x-master {string}
set security-8021x-mode [default|dynamic-vlan|...]
set security-exempt-list {string}
set security-external-logout {string}
set security-external-web {var-string}
set security-groups <name1>, <name2>, ...
set security-mac-auth-bypass [mac-auth-only|enable|...]
set security-mode [none|captive-portal|...]
set security-redirect-url {var-string}
set service-name {string}
set sflow-sampler [enable|disable]
set sfp-dsl [disable|enable]

```



```

set sfp-dsl-adsl-fallback [disable|enable]
set sfp-dsl-autodetect [disable|enable]
set sfp-dsl-mac {mac-address}
set snmp-index {integer}
set speed [auto|10full|...]
set spillover-threshold {integer}
set src-check [enable|disable]
set status [up|down]
set stp [disable|enable]
set stp-ha-secondary [disable|enable|...]
set stpforward [enable|disable]
set stpforward-mode [rpl-all-ext-id|rpl-bridge-ext-id|...]
set subst [enable|disable]
set substitute-dst-mac {mac-address}
set sw-algorithm [l2|l3|...]
set swc-first-create {integer}
set swc-vlan {integer}
set switch {string}
set switch-controller-access-vlan [enable|disable]
set switch-controller-arp-inspection [enable|disable]
set switch-controller-dhcp-snooping [enable|disable]
set switch-controller-dhcp-snooping-option82 [enable|disable]
set switch-controller-dhcp-snooping-verify-mac [enable|disable]
set switch-controller-dynamic {string}
set switch-controller-feature [none|default-vlan|...]
set switch-controller-igmp-snooping [enable|disable]
set switch-controller-igmp-snooping-fast-leave [enable|disable]
set switch-controller-igmp-snooping-proxy [enable|disable]
set switch-controller-iot-scanning [enable|disable]
set switch-controller-learning-limit {integer}
set switch-controller-mgmt-vlan {integer}
set switch-controller-nac {string}
set switch-controller-rspan-mode [disable|enable]
set switch-controller-source-ip [outbound|fixed]
set switch-controller-traffic-policy {string}
set system-id {mac-address}
set system-id-type [auto|user]
config tagging
    Description: Config object tagging.
    edit <name>
        set category {string}
        set tags <name1>, <name2>, ...
    next
end
set tc-mode {option}
set tcp-mss {integer}
set trunk [enable|disable]
set trust-ip-1 {ipv4-classnet-any}
set trust-ip-2 {ipv4-classnet-any}
set trust-ip-3 {ipv4-classnet-any}
set trust-ip6-1 {ipv6-prefix}
set trust-ip6-2 {ipv6-prefix}
set trust-ip6-3 {ipv6-prefix}
set type [physical|vlan|...]
set username {string}
set vci {integer}

```

```

set vdom {string}
set vectoring [disable|enable]
set vindex {integer}
set vlan-protocol [8021q|8021ad]
set vlanforward [enable|disable]
set vlanid {integer}
set vpi {integer}
set vrf {integer}
config vrrp
    Description: VRRP configuration.
    edit <vrid>
        set version [2|3]
        set vrgrp {integer}
        set vrip {ipv4-address-any}
        set priority {integer}
        set adv-interval {integer}
        set start-time {integer}
        set preempt [enable|disable]
        set accept-mode [enable|disable]
        set vrdest {ipv4-address-any}
        set vrdest-priority {integer}
        set ignore-default-route [enable|disable]
        set status [enable|disable]
        config proxy-arp
            Description: VRRP Proxy ARP configuration.
            edit <id>
                set ip {user}
            next
        end
    next
end
set vrrp-virtual-mac [enable|disable]
set wccp [enable|disable]
set weight {integer}
set wifi-5g-threshold {string}
set wifi-acl [allow|deny]
set wifi-ap-band [any|5g-preferred|...]
set wifi-auth [PSK|radius|...]
set wifi-auto-connect [enable|disable]
set wifi-auto-save [enable|disable]
set wifi-broadcast-ssid [enable|disable]
set wifi-encrypt [TKIP|AES]
set wifi-fragment-threshold {integer}
set wifi-key {password}
set wifi-keyindex {integer}
set wifi-mac-filter [enable|disable]
config wifi-mac-list
    Description: MAC filter list.
    edit <id>
        set mac {mac-address}
    next
end
config wifi-networks
    Description: WiFi network table.
    edit <id>
        set wifi-ssid {string}

```

```

        set wifi-security [open|wep64|...]
        set wifi-encrypt [TKIP|AES]
        set wifi-keyindex {integer}
        set wifi-key {password}
        set wifi-passphrase {password}
    next
end
set wifi-passphrase {password}
set wifi-radius-server {string}
set wifi-rts-threshold {integer}
set wifi-security [open|wep64|...]
set wifi-ssid {string}
set wifi-usergroup {string}
set wins-ip {ipv4-address}
next
end

```

## config system interface

Parameter	Description	Type	Size	Default												
ac-name	PPPoE server name.	string	Maximum length: 63													
aggregate	Aggregate interface.	string	Maximum length: 15													
algorithm	Frame distribution algorithm.	option	-	L4												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>L2</td><td>Use layer 2 address for distribution.</td></tr><tr><td>L3</td><td>Use layer 3 address for distribution.</td></tr><tr><td>L4</td><td>Use layer 4 information for distribution.</td></tr></table>				Option	Description	L2	Use layer 2 address for distribution.	L3	Use layer 3 address for distribution.	L4	Use layer 4 information for distribution.				
Option	Description															
L2	Use layer 2 address for distribution.															
L3	Use layer 3 address for distribution.															
L4	Use layer 4 information for distribution.															
alias	Alias will be displayed with the interface name to make it easier to distinguish.	string	Maximum length: 25													
allowaccess	Permitted types of management access to this interface.	option	-													
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ping</td><td>PING access.</td></tr><tr><td>https</td><td>HTTPS access.</td></tr><tr><td>ssh</td><td>SSH access.</td></tr><tr><td>snmp</td><td>SNMP access.</td></tr><tr><td>http</td><td>HTTP access.</td></tr></table>				Option	Description	ping	PING access.	https	HTTPS access.	ssh	SSH access.	snmp	SNMP access.	http	HTTP access.
Option	Description															
ping	PING access.															
https	HTTPS access.															
ssh	SSH access.															
snmp	SNMP access.															
http	HTTP access.															

Parameter	Description	Type	Size	Default																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>telnet</i></td><td>TELNET access.</td></tr><tr><td><i>fgfm</i></td><td>FortiManager access.</td></tr><tr><td><i>radius-acct</i></td><td>RADIUS accounting access.</td></tr><tr><td><i>probe-response</i></td><td>Probe access.</td></tr><tr><td><i>fabric</i></td><td>Security Fabric access.</td></tr><tr><td><i>ftm</i></td><td>FTM access.</td></tr><tr><td><i>speed-test</i></td><td>Speed test access.</td></tr></table>	Option	Description	<i>telnet</i>	TELNET access.	<i>fgfm</i>	FortiManager access.	<i>radius-acct</i>	RADIUS accounting access.	<i>probe-response</i>	Probe access.	<i>fabric</i>	Security Fabric access.	<i>ftm</i>	FTM access.	<i>speed-test</i>	Speed test access.			
	Option	Description																		
	<i>telnet</i>	TELNET access.																		
	<i>fgfm</i>	FortiManager access.																		
	<i>radius-acct</i>	RADIUS accounting access.																		
	<i>probe-response</i>	Probe access.																		
	<i>fabric</i>	Security Fabric access.																		
	<i>ftm</i>	FTM access.																		
<i>speed-test</i>	Speed test access.																			
ap-discover	Enable/disable automatic registration of unknown FortiAP devices.	option	-	enable																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable automatic registration of unknown FortiAP devices.</td></tr><tr><td><i>disable</i></td><td>Disable automatic registration of unknown FortiAP devices.</td></tr></table>	Option	Description	<i>enable</i>	Enable automatic registration of unknown FortiAP devices.	<i>disable</i>	Disable automatic registration of unknown FortiAP devices.													
	Option	Description																		
	<i>enable</i>	Enable automatic registration of unknown FortiAP devices.																		
<i>disable</i>	Disable automatic registration of unknown FortiAP devices.																			
arpforward	Enable/disable ARP forwarding.	option	-	enable																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable ARP forwarding.</td></tr><tr><td><i>disable</i></td><td>Disable ARP forwarding.</td></tr></table>	Option	Description	<i>enable</i>	Enable ARP forwarding.	<i>disable</i>	Disable ARP forwarding.													
	Option	Description																		
	<i>enable</i>	Enable ARP forwarding.																		
<i>disable</i>	Disable ARP forwarding.																			
atm-protocol *	ATM protocol.	option	-	none																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>Not over ATM.</td></tr><tr><td><i>ipoa</i></td><td>IPoA RFC2684.</td></tr></table>	Option	Description	<i>none</i>	Not over ATM.	<i>ipoa</i>	IPoA RFC2684.													
	Option	Description																		
	<i>none</i>	Not over ATM.																		
<i>ipoa</i>	IPoA RFC2684.																			
auth-cert	HTTPS server certificate.	string	Maximum length: 35																	
auth-portal-addr	Address of captive portal.	string	Maximum length: 63																	
auth-type	PPP authentication type to use.	option	-	auto																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto</i></td><td>Automatically choose authentication.</td></tr><tr><td><i>pap</i></td><td>PAP authentication.</td></tr></table>	Option	Description	<i>auto</i>	Automatically choose authentication.	<i>pap</i>	PAP authentication.													
	Option	Description																		
	<i>auto</i>	Automatically choose authentication.																		
<i>pap</i>	PAP authentication.																			

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>chap</i></td><td>CHAP authentication.</td></tr><tr><td><i>mschapv1</i></td><td>MS-CHAPv1 authentication.</td></tr><tr><td><i>mschapv2</i></td><td>MS-CHAPv2 authentication.</td></tr></table>	Option	Description	<i>chap</i>	CHAP authentication.	<i>mschapv1</i>	MS-CHAPv1 authentication.	<i>mschapv2</i>	MS-CHAPv2 authentication.			
	Option	Description										
	<i>chap</i>	CHAP authentication.										
	<i>mschapv1</i>	MS-CHAPv1 authentication.										
<i>mschapv2</i>	MS-CHAPv2 authentication.											
auto-auth-extension-device	Enable/disable automatic authorization of dedicated Fortinet extension device on this interface.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable automatic authorization of dedicated Fortinet extension device on this interface.</td></tr><tr><td><i>disable</i></td><td>Disable automatic authorization of dedicated Fortinet extension device on this interface.</td></tr></table>	Option	Description	<i>enable</i>	Enable automatic authorization of dedicated Fortinet extension device on this interface.	<i>disable</i>	Disable automatic authorization of dedicated Fortinet extension device on this interface.					
	Option	Description										
	<i>enable</i>	Enable automatic authorization of dedicated Fortinet extension device on this interface.										
<i>disable</i>	Disable automatic authorization of dedicated Fortinet extension device on this interface.											
bandwidth-measure-time	Bandwidth measure time.	integer	Minimum value: 0 Maximum value: 4294967295	0								
bfd	Bidirectional Forwarding Detection (BFD) settings.	option	-	global								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>global</i></td><td>BFD behavior of this interface will be based on global configuration.</td></tr><tr><td><i>enable</i></td><td>Enable BFD on this interface and ignore global configuration.</td></tr><tr><td><i>disable</i></td><td>Disable BFD on this interface and ignore global configuration.</td></tr></table>	Option	Description	<i>global</i>	BFD behavior of this interface will be based on global configuration.	<i>enable</i>	Enable BFD on this interface and ignore global configuration.	<i>disable</i>	Disable BFD on this interface and ignore global configuration.			
	Option	Description										
	<i>global</i>	BFD behavior of this interface will be based on global configuration.										
	<i>enable</i>	Enable BFD on this interface and ignore global configuration.										
<i>disable</i>	Disable BFD on this interface and ignore global configuration.											
bfd-desired-min-tx	BFD desired minimal transmit interval.	integer	Minimum value: 1 Maximum value: 100000	250								
bfd-detect-mult	BFD detection multiplier.	integer	Minimum value: 1 Maximum value: 50	3								
bfd-required-min-rx	BFD required minimal receive interval.	integer	Minimum value: 1 Maximum value: 100000	250								

Parameter	Description	Type	Size	Default						
broadcast-forward	Enable/disable broadcast forwarding.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable broadcast forwarding.</td></tr><tr><td><i>disable</i></td><td>Disable broadcast forwarding.</td></tr></table>				Option	Description	<i>enable</i>	Enable broadcast forwarding.	<i>disable</i>	Disable broadcast forwarding.
	Option	Description								
	<i>enable</i>	Enable broadcast forwarding.								
<i>disable</i>	Disable broadcast forwarding.									
cli-conn-status	CLI connection status.	integer	Minimum value: 0 Maximum value: 4294967295	0						
color	Color of icon on the GUI.	integer	Minimum value: 0 Maximum value: 32	0						
dedicated-to	Configure interface for single purpose.	option	-	none						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>Interface not dedicated for any purpose.</td></tr><tr><td><i>management</i></td><td>Dedicate this interface for management purposes only.</td></tr></table>				Option	Description	<i>none</i>	Interface not dedicated for any purpose.	<i>management</i>	Dedicate this interface for management purposes only.
	Option	Description								
	<i>none</i>	Interface not dedicated for any purpose.								
<i>management</i>	Dedicate this interface for management purposes only.									
defaultgw	Enable to get the gateway IP from the DHCP or PPPoE server.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable default gateway.</td></tr><tr><td><i>disable</i></td><td>Disable default gateway.</td></tr></table>				Option	Description	<i>enable</i>	Enable default gateway.	<i>disable</i>	Disable default gateway.
	Option	Description								
	<i>enable</i>	Enable default gateway.								
<i>disable</i>	Disable default gateway.									
description	Description.	var-string	Maximum length: 255							
detected-peer-mtu	MTU of detected peer.	integer	Minimum value: 0 Maximum value: 4294967295	0						
detectprotocol	Protocols used to detect the server.	option	-	ping						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ping</i></td><td>PING.</td></tr></table>				Option	Description	<i>ping</i>	PING.		
	Option	Description								
<i>ping</i>	PING.									

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>tcp-echo</i></td><td>TCP echo.</td></tr><tr><td><i>udp-echo</i></td><td>UDP echo.</td></tr></table>	Option	Description	<i>tcp-echo</i>	TCP echo.	<i>udp-echo</i>	UDP echo.			
	Option	Description								
	<i>tcp-echo</i>	TCP echo.								
<i>udp-echo</i>	UDP echo.									
detectserver	Gateway's ping server for this IP.	user	Not Specified							
device-identification	Enable/disable passively gathering of device identity information about the devices on the network connected to this interface.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable passive gathering of identity information about hosts.</td></tr><tr><td><i>disable</i></td><td>Disable passive gathering of identity information about hosts.</td></tr></table>	Option	Description	<i>enable</i>	Enable passive gathering of identity information about hosts.	<i>disable</i>	Disable passive gathering of identity information about hosts.			
	Option	Description								
	<i>enable</i>	Enable passive gathering of identity information about hosts.								
<i>disable</i>	Disable passive gathering of identity information about hosts.									
device-user-identification	Enable/disable passive gathering of user identity information about users on this interface.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable passive gathering of user identity information about users.</td></tr><tr><td><i>disable</i></td><td>Disable passive gathering of user identity information about users.</td></tr></table>	Option	Description	<i>enable</i>	Enable passive gathering of user identity information about users.	<i>disable</i>	Disable passive gathering of user identity information about users.			
	Option	Description								
	<i>enable</i>	Enable passive gathering of user identity information about users.								
<i>disable</i>	Disable passive gathering of user identity information about users.									
devindex	Device Index.	integer	Minimum value: 0 Maximum value: 4294967295	0						
dhcp-classless-route-addition	Enable/disable addition of classless static routes retrieved from DHCP server.	option	-	disable **						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable addition of classless static routes retrieved from DHCP server.</td></tr><tr><td><i>disable</i></td><td>Disable addition of classless static routes retrieved from DHCP server.</td></tr></table>	Option	Description	<i>enable</i>	Enable addition of classless static routes retrieved from DHCP server.	<i>disable</i>	Disable addition of classless static routes retrieved from DHCP server.			
	Option	Description								
	<i>enable</i>	Enable addition of classless static routes retrieved from DHCP server.								
<i>disable</i>	Disable addition of classless static routes retrieved from DHCP server.									
dhcp-client-identifier	DHCP client identifier.	string	Maximum length: 48							
dhcp-relay-agent-option	Enable/disable DHCP relay agent option.	option	-	enable						

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable DHCP relay agent option.		
	<i>disable</i>	Disable DHCP relay agent option.		
dhcp-relay-interface	Specify outgoing interface to reach server.	string	Maximum length: 15	
dhcp-relay-interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto
	<b>Option</b>	<b>Description</b>		
	<i>auto</i>	Set outgoing interface automatically.		
	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.		
	<i>specify</i>	Set outgoing interface manually.		
dhcp-relay-ip	DHCP relay IP address.	user	Not Specified	
dhcp-relay-link-selection	DHCP relay link selection.	ipv4-address	Not Specified	0.0.0.0
dhcp-relay-request-all-server	Enable/disable sending of DHCP requests to all servers.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Send DHCP requests only to a matching server.		
	<i>enable</i>	Send DHCP requests to all servers.		
dhcp-relay-service	Enable/disable allowing this interface to act as a DHCP relay.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	None.		
	<i>enable</i>	DHCP relay agent.		
dhcp-relay-type	DHCP relay type (regular or IPsec).	option	-	regular
	<b>Option</b>	<b>Description</b>		
	<i>regular</i>	Regular DHCP relay.		
	<i>ipsec</i>	DHCP relay for IPsec.		



Parameter	Description	Type	Size	Default								
dhcp-renew-time	DHCP renew time in seconds , 0 means use the renew time provided by the server.	integer	Minimum value: 300 Maximum value: 604800	0								
disc-retry-timeout	Time in seconds to wait before retrying to start a PPPoE discovery, 0 means no timeout.	integer	Minimum value: 0 Maximum value: 4294967295	1								
disconnect-threshold	Time in milliseconds to wait before sending a notification that this interface is down or disconnected.	integer	Minimum value: 0 Maximum value: 10000	0								
distance	Distance for routes learned through PPPoE or DHCP, lower distance indicates preferred route.	integer	Minimum value: 1 Maximum value: 255	5								
dns-server-override	Enable/disable use DNS acquired by DHCP or PPPoE.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Use DNS acquired by DHCP or PPPoE.</td></tr><tr><td><i>disable</i></td><td>No not use DNS acquired by DHCP or PPPoE.</td></tr></table>				Option	Description	<i>enable</i>	Use DNS acquired by DHCP or PPPoE.	<i>disable</i>	No not use DNS acquired by DHCP or PPPoE.		
Option	Description											
<i>enable</i>	Use DNS acquired by DHCP or PPPoE.											
<i>disable</i>	No not use DNS acquired by DHCP or PPPoE.											
dns-server-protocol	DNS transport protocols.	option	-	cleartext								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>cleartext</i></td><td>DNS over UDP/53, DNS over TCP/53.</td></tr><tr><td><i>dot</i></td><td>DNS over TLS/853.</td></tr><tr><td><i>doh</i></td><td>DNS over HTTPS/443.</td></tr></table>				Option	Description	<i>cleartext</i>	DNS over UDP/53, DNS over TCP/53.	<i>dot</i>	DNS over TLS/853.	<i>doh</i>	DNS over HTTPS/443.
Option	Description											
<i>cleartext</i>	DNS over UDP/53, DNS over TCP/53.											
<i>dot</i>	DNS over TLS/853.											
<i>doh</i>	DNS over HTTPS/443.											
drop-fragment	Enable/disable drop fragment packets.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable/disable drop fragment packets.</td></tr><tr><td><i>disable</i></td><td>Do not drop fragment packets.</td></tr></table>				Option	Description	<i>enable</i>	Enable/disable drop fragment packets.	<i>disable</i>	Do not drop fragment packets.		
Option	Description											
<i>enable</i>	Enable/disable drop fragment packets.											
<i>disable</i>	Do not drop fragment packets.											
drop-overlapped-fragment	Enable/disable drop overlapped fragment packets.	option	-	disable								

Parameter	Description	Type	Size	Default																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable drop of overlapped fragment packets.</td></tr><tr><td><i>disable</i></td><td>Disable drop of overlapped fragment packets.</td></tr></table>	Option	Description	<i>enable</i>	Enable drop of overlapped fragment packets.	<i>disable</i>	Disable drop of overlapped fragment packets.																	
	Option	Description																						
	<i>enable</i>	Enable drop of overlapped fragment packets.																						
<i>disable</i>	Disable drop of overlapped fragment packets.																							
egress-cos *	Override outgoing CoS in user VLAN tag.	option	-	disable																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable.</td></tr><tr><td><i>cos0</i></td><td>CoS 0.</td></tr><tr><td><i>cos1</i></td><td>CoS 1.</td></tr><tr><td><i>cos2</i></td><td>CoS 2.</td></tr><tr><td><i>cos3</i></td><td>CoS 3.</td></tr><tr><td><i>cos4</i></td><td>CoS 4.</td></tr><tr><td><i>cos5</i></td><td>CoS 5.</td></tr><tr><td><i>cos6</i></td><td>CoS 6.</td></tr><tr><td><i>cos7</i></td><td>CoS 7.</td></tr></table>	Option	Description	<i>disable</i>	Disable.	<i>cos0</i>	CoS 0.	<i>cos1</i>	CoS 1.	<i>cos2</i>	CoS 2.	<i>cos3</i>	CoS 3.	<i>cos4</i>	CoS 4.	<i>cos5</i>	CoS 5.	<i>cos6</i>	CoS 6.	<i>cos7</i>	CoS 7.			
	Option	Description																						
	<i>disable</i>	Disable.																						
	<i>cos0</i>	CoS 0.																						
	<i>cos1</i>	CoS 1.																						
	<i>cos2</i>	CoS 2.																						
	<i>cos3</i>	CoS 3.																						
	<i>cos4</i>	CoS 4.																						
	<i>cos5</i>	CoS 5.																						
<i>cos6</i>	CoS 6.																							
<i>cos7</i>	CoS 7.																							
egress-shaping-profile	Outgoing traffic shaping profile.	string	Maximum length: 35																					
estimated-downstream-bandwidth	Estimated maximum downstream bandwidth (kbps). Used to estimate link utilization.	integer	Minimum value: 0 Maximum value: 4294967295	0																				
estimated-upstream-bandwidth	Estimated maximum upstream bandwidth (kbps). Used to estimate link utilization.	integer	Minimum value: 0 Maximum value: 4294967295	0																				
explicit-ftp-proxy	Enable/disable the explicit FTP proxy on this interface.	option	-	disable																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable explicit FTP proxy on this interface.</td></tr><tr><td><i>disable</i></td><td>Disable explicit FTP proxy on this interface.</td></tr></table>	Option	Description	<i>enable</i>	Enable explicit FTP proxy on this interface.	<i>disable</i>	Disable explicit FTP proxy on this interface.																	
	Option	Description																						
	<i>enable</i>	Enable explicit FTP proxy on this interface.																						
<i>disable</i>	Disable explicit FTP proxy on this interface.																							
explicit-web-proxy	Enable/disable the explicit web proxy on this interface.	option	-	disable																				

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable explicit Web proxy on this interface.</td></tr><tr><td><i>disable</i></td><td>Disable explicit Web proxy on this interface.</td></tr></table>	Option	Description	<i>enable</i>	Enable explicit Web proxy on this interface.	<i>disable</i>	Disable explicit Web proxy on this interface.					
	Option	Description										
	<i>enable</i>	Enable explicit Web proxy on this interface.										
<i>disable</i>	Disable explicit Web proxy on this interface.											
external	Enable/disable identifying the interface as an external interface (which usually means it's connected to the Internet).	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable identifying the interface as an external interface.</td></tr><tr><td><i>disable</i></td><td>Disable identifying the interface as an external interface.</td></tr></table>	Option	Description	<i>enable</i>	Enable identifying the interface as an external interface.	<i>disable</i>	Disable identifying the interface as an external interface.					
	Option	Description										
	<i>enable</i>	Enable identifying the interface as an external interface.										
<i>disable</i>	Disable identifying the interface as an external interface.											
fail-action-on-extender	Action on FortiExtender when interface fail.	option	-	soft-restart								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>soft-restart</i></td><td>Soft-restart-on-extender.</td></tr><tr><td><i>hard-restart</i></td><td>Hard-restart-on-extender.</td></tr><tr><td><i>reboot</i></td><td>Reboot-on-extender.</td></tr></table>	Option	Description	<i>soft-restart</i>	Soft-restart-on-extender.	<i>hard-restart</i>	Hard-restart-on-extender.	<i>reboot</i>	Reboot-on-extender.			
	Option	Description										
	<i>soft-restart</i>	Soft-restart-on-extender.										
	<i>hard-restart</i>	Hard-restart-on-extender.										
<i>reboot</i>	Reboot-on-extender.											
fail-alert-interfaces <name>	Names of the FortiGate interfaces to which the link failure alert is sent. Names of the non-virtual interface.	string	Maximum length: 79									
fail-alert-method	Select link-failed-signal or link-down method to alert about a failed link.	option	-	link-down								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>link-failed-signal</i></td><td>Link-failed-signal.</td></tr><tr><td><i>link-down</i></td><td>Link-down.</td></tr></table>	Option	Description	<i>link-failed-signal</i>	Link-failed-signal.	<i>link-down</i>	Link-down.					
	Option	Description										
	<i>link-failed-signal</i>	Link-failed-signal.										
<i>link-down</i>	Link-down.											
fail-detect	Enable/disable fail detection features for this interface.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable interface failed option status.</td></tr><tr><td><i>disable</i></td><td>Disable interface failed option status.</td></tr></table>	Option	Description	<i>enable</i>	Enable interface failed option status.	<i>disable</i>	Disable interface failed option status.					
	Option	Description										
	<i>enable</i>	Enable interface failed option status.										
<i>disable</i>	Disable interface failed option status.											
fail-detect-option	Options for detecting that this interface has failed.	option	-	link-down								

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>detectserver</i></td><td>Use a ping server to determine if the interface has failed.</td></tr><tr><td><i>link-down</i></td><td>Use port detection to determine if the interface has failed.</td></tr></table>				Option	Description	<i>detectserver</i>	Use a ping server to determine if the interface has failed.	<i>link-down</i>	Use port detection to determine if the interface has failed.
	Option	Description								
	<i>detectserver</i>	Use a ping server to determine if the interface has failed.								
<i>link-down</i>	Use port detection to determine if the interface has failed.									
fortilink *	Enable FortiLink to dedicate this interface to manage other Fortinet devices.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable FortiLink to dedicated interface for managing FortiSwitch devices.</td></tr><tr><td><i>disable</i></td><td>Disable FortiLink to dedicated interface for managing FortiSwitch devices.</td></tr></table>				Option	Description	<i>enable</i>	Enable FortiLink to dedicated interface for managing FortiSwitch devices.	<i>disable</i>	Disable FortiLink to dedicated interface for managing FortiSwitch devices.
	Option	Description								
	<i>enable</i>	Enable FortiLink to dedicated interface for managing FortiSwitch devices.								
<i>disable</i>	Disable FortiLink to dedicated interface for managing FortiSwitch devices.									
fortilink-backup-link	FortiLink split interface backup link.	integer	Minimum value: 0 Maximum value: 255	0						
fortilink-neighbor-detect	Protocol for FortiGate neighbor discovery.	option	-	fortilink						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>lldp</i></td><td>Detect FortiLink neighbors using LLDP protocol.</td></tr><tr><td><i>fortilink</i></td><td>Detect FortiLink neighbors using FortiLink protocol.</td></tr></table>				Option	Description	<i>lldp</i>	Detect FortiLink neighbors using LLDP protocol.	<i>fortilink</i>	Detect FortiLink neighbors using FortiLink protocol.
	Option	Description								
	<i>lldp</i>	Detect FortiLink neighbors using LLDP protocol.								
<i>fortilink</i>	Detect FortiLink neighbors using FortiLink protocol.									
fortilink-split-interface	Enable/disable FortiLink split interface to connect member link to different FortiSwitch in stack for uplink redundancy.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable FortiLink split interface to connect member link to different FortiSwitch in stack for uplink redundancy.</td></tr><tr><td><i>disable</i></td><td>Disable FortiLink split interface.</td></tr></table>				Option	Description	<i>enable</i>	Enable FortiLink split interface to connect member link to different FortiSwitch in stack for uplink redundancy.	<i>disable</i>	Disable FortiLink split interface.
	Option	Description								
	<i>enable</i>	Enable FortiLink split interface to connect member link to different FortiSwitch in stack for uplink redundancy.								
<i>disable</i>	Disable FortiLink split interface.									
forward-domain	Transparent mode forward domain.	integer	Minimum value: 0 Maximum value: 2147483647	0						
forward-error-correction *	Configure forward error correction (FEC).	option	-	none						

Parameter	Description	Type	Size	Default
	<div><div>Option</div><div>Description</div></div>			
	none	none		
	disable	Disable forward error correction (FEC).		
	cl91-rs-fec	Reed-Solomon (FEC CL91).		
	cl74-fc-fec	Fire-Code (FEC CL74).		
gateway-address *	Gateway address	ipv4-address	Not Specified	0.0.0.0
gi-gk *	Enable/disable Gi Gatekeeper.	option	-	disable
	<div><div>Option</div><div>Description</div></div>			
	enable	enable Gi Gatekeeper		
	disable	disable Gi Gatekeeper		
gwaddr *	Gateway address	ipv4-address	Not Specified	0.0.0.0
gwdetect	Enable/disable detect gateway alive for first.	option	-	disable
	<div><div>Option</div><div>Description</div></div>			
	enable	Enable detect gateway alive for first.		
	disable	Disable detect gateway alive for first.		
ha-priority	HA election priority for the PING server.	integer	Minimum value: 1 Maximum value: 50	1
icmp-accept-redirect	Enable/disable ICMP accept redirect.	option	-	enable
	<div><div>Option</div><div>Description</div></div>			
	enable	Enable ICMP accept redirect.		
	disable	Disable ICMP accept redirect.		
icmp-send-redirect	Enable/disable sending of ICMP redirects.	option	-	enable

Parameter	Description	Type	Size	Default																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable sending of ICMP redirects.</td></tr><tr><td><i>disable</i></td><td>Disable sending of ICMP redirects.</td></tr></table>	Option	Description	<i>enable</i>	Enable sending of ICMP redirects.	<i>disable</i>	Disable sending of ICMP redirects.																	
	Option	Description																						
	<i>enable</i>	Enable sending of ICMP redirects.																						
<i>disable</i>	Disable sending of ICMP redirects.																							
ident-accept	Enable/disable authentication for this interface.	option	-	disable																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable determining a user's identity from packet identification.</td></tr><tr><td><i>disable</i></td><td>Disable determining a user's identity from packet identification.</td></tr></table>	Option	Description	<i>enable</i>	Enable determining a user's identity from packet identification.	<i>disable</i>	Disable determining a user's identity from packet identification.																	
	Option	Description																						
	<i>enable</i>	Enable determining a user's identity from packet identification.																						
<i>disable</i>	Disable determining a user's identity from packet identification.																							
idle-timeout	PPPoE auto disconnect after idle timeout seconds, 0 means no timeout.	integer	Minimum value: 0 Maximum value: 32767	0																				
inbandwidth	Bandwidth limit for incoming traffic , 0 means unlimited.	integer	Minimum value: 0 Maximum value: 80000000 **	0																				
ingress-cos *	Override incoming CoS in user VLAN tag on VLAN interface or assign a priority VLAN tag on physical interface.	option	-	disable																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable.</td></tr><tr><td><i>cos0</i></td><td>CoS 0.</td></tr><tr><td><i>cos1</i></td><td>CoS 1.</td></tr><tr><td><i>cos2</i></td><td>CoS 2.</td></tr><tr><td><i>cos3</i></td><td>CoS 3.</td></tr><tr><td><i>cos4</i></td><td>CoS 4.</td></tr><tr><td><i>cos5</i></td><td>CoS 5.</td></tr><tr><td><i>cos6</i></td><td>CoS 6.</td></tr><tr><td><i>cos7</i></td><td>CoS 7.</td></tr></table>	Option	Description	<i>disable</i>	Disable.	<i>cos0</i>	CoS 0.	<i>cos1</i>	CoS 1.	<i>cos2</i>	CoS 2.	<i>cos3</i>	CoS 3.	<i>cos4</i>	CoS 4.	<i>cos5</i>	CoS 5.	<i>cos6</i>	CoS 6.	<i>cos7</i>	CoS 7.			
	Option	Description																						
	<i>disable</i>	Disable.																						
	<i>cos0</i>	CoS 0.																						
	<i>cos1</i>	CoS 1.																						
	<i>cos2</i>	CoS 2.																						
	<i>cos3</i>	CoS 3.																						
	<i>cos4</i>	CoS 4.																						
	<i>cos5</i>	CoS 5.																						
	<i>cos6</i>	CoS 6.																						
<i>cos7</i>	CoS 7.																							
ingress-shaping-profile	Incoming traffic shaping profile.	string	Maximum length: 35																					

Parameter	Description	Type	Size	Default
ingress-spillover-threshold	Ingress Spillover threshold , 0 means unlimited.	integer	Minimum value: 0 Maximum value: 16776000	0
interface	Interface name.	string	Maximum length: 15	
internal	Implicitly created.	integer	Minimum value: 0 Maximum value: 255	0
ip	Interface IPv4 address and subnet mask, syntax: X.X.X.X/24.	ipv4-classnet-host	Not Specified	0.0.0.0 0.0.0.0
ip-managed-by-fortipam	Enable/disable automatic IP address assignment of this interface by FortiPAM.	option	-	disable
	<b>Option</b>		<b>Description</b>	
	<i>enable</i>		Enable automatic IP address assignment of this interface by FortiPAM.	
	<i>disable</i>		Disable automatic IP address assignment of this interface by FortiPAM.	
ipmac	Enable/disable IP/MAC binding.	option	-	disable
	<b>Option</b>		<b>Description</b>	
	<i>enable</i>		Enable IP/MAC binding.	
	<i>disable</i>		Disable IP/MAC binding.	
ips-sniffer-mode	Enable/disable the use of this interface as a one-armed sniffer.	option	-	disable
	<b>Option</b>		<b>Description</b>	
	<i>enable</i>		Enable IPS sniffer mode.	
	<i>disable</i>		Disable IPS sniffer mode.	
ipunnumbered	Unnumbered IP used for PPPoE interfaces for which no unique local address is provided.	ipv4-address	Not Specified	0.0.0.0
l2forward	Enable/disable l2 forwarding.	option	-	disable

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable L2 forwarding.		
	<i>disable</i>	Disable L2 forwarding.		
l2tp-client *	Enable/disable this interface as a Layer 2 Tunneling Protocol (L2TP) client.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable L2TP client.		
	<i>disable</i>	Disable L2TP client.		
lacp-ha-slave	LACP HA slave.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Allow HA slave to send/receive LACP messages.		
	<i>disable</i>	Block HA slave from sending/receiving LACP messages.		
lacp-mode	LACP mode.	option	-	active
	<b>Option</b>	<b>Description</b>		
	<i>static</i>	Use static aggregation, do not send and ignore any LACP messages.		
	<i>passive</i>	Passively use LACP to negotiate 802.3ad aggregation.		
	<i>active</i>	Actively use LACP to negotiate 802.3ad aggregation.		
lacp-speed	How often the interface sends LACP messages.	option	-	slow
	<b>Option</b>	<b>Description</b>		
	<i>slow</i>	Send LACP message every 30 seconds.		
	<i>fast</i>	Send LACP message every second.		
lcp-echo-interval	Time in seconds between PPPoE Link Control Protocol (LCP) echo requests.	integer	Minimum value: 0 Maximum value: 32767	5
lcp-max-echo-fails	Maximum missed LCP echo messages before disconnect.	integer	Minimum value: 0 Maximum value: 32767	3



Parameter	Description	Type	Size	Default														
link-up-delay	Number of milliseconds to wait before considering a link is up.	integer	Minimum value: 50 Maximum value: 3600000	50														
lldp-network-policy	LLDP-MED network policy profile.	string	Maximum length: 35															
lldp-reception	Enable/disable Link Layer Discovery Protocol (LLDP) reception.	option	-	vdom														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable reception of Link Layer Discovery Protocol (LLDP).</td></tr><tr><td>disable</td><td>Disable reception of Link Layer Discovery Protocol (LLDP).</td></tr><tr><td>vdom</td><td>Use VDOM Link Layer Discovery Protocol (LLDP) reception configuration setting.</td></tr></table>				Option	Description	enable	Enable reception of Link Layer Discovery Protocol (LLDP).	disable	Disable reception of Link Layer Discovery Protocol (LLDP).	vdom	Use VDOM Link Layer Discovery Protocol (LLDP) reception configuration setting.						
Option	Description																	
enable	Enable reception of Link Layer Discovery Protocol (LLDP).																	
disable	Disable reception of Link Layer Discovery Protocol (LLDP).																	
vdom	Use VDOM Link Layer Discovery Protocol (LLDP) reception configuration setting.																	
lldp-transmission	Enable/disable Link Layer Discovery Protocol (LLDP) transmission.	option	-	vdom														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable transmission of Link Layer Discovery Protocol (LLDP).</td></tr><tr><td>disable</td><td>Disable transmission of Link Layer Discovery Protocol (LLDP).</td></tr><tr><td>vdom</td><td>Use VDOM Link Layer Discovery Protocol (LLDP) transmission configuration setting.</td></tr></table>				Option	Description	enable	Enable transmission of Link Layer Discovery Protocol (LLDP).	disable	Disable transmission of Link Layer Discovery Protocol (LLDP).	vdom	Use VDOM Link Layer Discovery Protocol (LLDP) transmission configuration setting.						
Option	Description																	
enable	Enable transmission of Link Layer Discovery Protocol (LLDP).																	
disable	Disable transmission of Link Layer Discovery Protocol (LLDP).																	
vdom	Use VDOM Link Layer Discovery Protocol (LLDP) transmission configuration setting.																	
macaddr	Change the interface's MAC address.	mac-address	Not Specified	00:00:00:00:00:00 **														
managed-subnetwork-size	Number of IP addresses to be allocated by FortiIPAM and used by this FortiGate unit's DHCP server settings.	option	-	256														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>32</td><td>Allocate a subnet with 32 IP addresses.</td></tr><tr><td>64</td><td>Allocate a subnet with 64 IP addresses.</td></tr><tr><td>128</td><td>Allocate a subnet with 128 IP addresses.</td></tr><tr><td>256</td><td>Allocate a subnet with 256 IP addresses.</td></tr><tr><td>512</td><td>Allocate a subnet with 512 IP addresses.</td></tr><tr><td>1024</td><td>Allocate a subnet with 1024 IP addresses.</td></tr></table>				Option	Description	32	Allocate a subnet with 32 IP addresses.	64	Allocate a subnet with 64 IP addresses.	128	Allocate a subnet with 128 IP addresses.	256	Allocate a subnet with 256 IP addresses.	512	Allocate a subnet with 512 IP addresses.	1024	Allocate a subnet with 1024 IP addresses.
Option	Description																	
32	Allocate a subnet with 32 IP addresses.																	
64	Allocate a subnet with 64 IP addresses.																	
128	Allocate a subnet with 128 IP addresses.																	
256	Allocate a subnet with 256 IP addresses.																	
512	Allocate a subnet with 512 IP addresses.																	
1024	Allocate a subnet with 1024 IP addresses.																	

Parameter	Description	Type	Size	Default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>2048</td><td>Allocate a subnet with 2048 IP addresses.</td></tr><tr><td>4096</td><td>Allocate a subnet with 4096 IP addresses.</td></tr><tr><td>8192</td><td>Allocate a subnet with 8192 IP addresses.</td></tr><tr><td>16384</td><td>Allocate a subnet with 16384 IP addresses.</td></tr><tr><td>32768</td><td>Allocate a subnet with 32768 IP addresses.</td></tr><tr><td>65536</td><td>Allocate a subnet with 65536 IP addresses.</td></tr></table>				Option	Description	2048	Allocate a subnet with 2048 IP addresses.	4096	Allocate a subnet with 4096 IP addresses.	8192	Allocate a subnet with 8192 IP addresses.	16384	Allocate a subnet with 16384 IP addresses.	32768	Allocate a subnet with 32768 IP addresses.	65536	Allocate a subnet with 65536 IP addresses.
	Option	Description																
	2048	Allocate a subnet with 2048 IP addresses.																
	4096	Allocate a subnet with 4096 IP addresses.																
	8192	Allocate a subnet with 8192 IP addresses.																
	16384	Allocate a subnet with 16384 IP addresses.																
	32768	Allocate a subnet with 32768 IP addresses.																
65536	Allocate a subnet with 65536 IP addresses.																	
management-ip	High Availability in-band management IP address of this interface.	ipv4-classnet-host	Not Specified	0.0.0.0 0.0.0.0														
measured-downstream-bandwidth	Measured downstream bandwidth (kbps).	integer	Minimum value: 0 Maximum value: 4294967295	0														
measured-upstream-bandwidth	Measured upstream bandwidth (kbps).	integer	Minimum value: 0 Maximum value: 4294967295	0														
mediatype *	Select SFP media interface type	option	-	serdes-sfp														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>serdes-sfp</td><td>SFP using SerDes Media Interface</td></tr><tr><td>sgmii-sfp</td><td>SFP using SGMII Media Interface</td></tr><tr><td>serdes-copper-sfp</td><td>Copper SFP using SerDes media Interface.</td></tr></table>				Option	Description	serdes-sfp	SFP using SerDes Media Interface	sgmii-sfp	SFP using SGMII Media Interface	serdes-copper-sfp	Copper SFP using SerDes media Interface.						
	Option	Description																
	serdes-sfp	SFP using SerDes Media Interface																
	sgmii-sfp	SFP using SGMII Media Interface																
serdes-copper-sfp	Copper SFP using SerDes media Interface.																	
member <interface-name>	Physical interfaces that belong to the aggregate or redundant interface. Physical interface name.	string	Maximum length: 79															
min-links	Minimum number of aggregated ports that must be up.	integer	Minimum value: 1 Maximum value: 32	1														
min-links-down	Action to take when less than the configured minimum number of links are active.	option	-	operational														

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>operational</i></td><td>Set the aggregate operationally down.</td></tr><tr><td><i>administrative</i></td><td>Set the aggregate administratively down.</td></tr></table>	Option	Description	<i>operational</i>	Set the aggregate operationally down.	<i>administrative</i>	Set the aggregate administratively down.					
	Option	Description										
	<i>operational</i>	Set the aggregate operationally down.										
<i>administrative</i>	Set the aggregate administratively down.											
mode	Addressing mode (static, DHCP, PPPoE).	option	-	static								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>static</i></td><td>Static setting.</td></tr><tr><td><i>dhcp</i></td><td>External DHCP client mode.</td></tr><tr><td><i>pppoe</i></td><td>External PPPoE mode.</td></tr></table>	Option	Description	<i>static</i>	Static setting.	<i>dhcp</i>	External DHCP client mode.	<i>pppoe</i>	External PPPoE mode.			
	Option	Description										
	<i>static</i>	Static setting.										
	<i>dhcp</i>	External DHCP client mode.										
<i>pppoe</i>	External PPPoE mode.											
monitor-bandwidth	Enable monitoring bandwidth on this interface.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable monitoring bandwidth on this interface.</td></tr><tr><td><i>disable</i></td><td>Disable monitoring bandwidth on this interface.</td></tr></table>	Option	Description	<i>enable</i>	Enable monitoring bandwidth on this interface.	<i>disable</i>	Disable monitoring bandwidth on this interface.					
	Option	Description										
	<i>enable</i>	Enable monitoring bandwidth on this interface.										
<i>disable</i>	Disable monitoring bandwidth on this interface.											
mtu	MTU value for this interface.	integer	Minimum value: 0 Maximum value: 4294967295	1500								
mtu-override	Enable to set a custom MTU for this interface.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Override default MTU.</td></tr><tr><td><i>disable</i></td><td>Use default MTU.</td></tr></table>	Option	Description	<i>enable</i>	Override default MTU.	<i>disable</i>	Use default MTU.					
	Option	Description										
	<i>enable</i>	Override default MTU.										
<i>disable</i>	Use default MTU.											
mux-type *	Multiplexer type	option	-	llc-encaps								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>llc-encaps</i></td><td>LLC encapsulation.</td></tr><tr><td><i>vc-encaps</i></td><td>VC encapsulation.</td></tr></table>	Option	Description	<i>llc-encaps</i>	LLC encapsulation.	<i>vc-encaps</i>	VC encapsulation.					
	Option	Description										
	<i>llc-encaps</i>	LLC encapsulation.										
<i>vc-encaps</i>	VC encapsulation.											
name	Name.	string	Maximum length: 15									
ndiscforward	Enable/disable NDISC forwarding.	option	-	enable								

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable NDISC forwarding.		
	<i>disable</i>	Disable NDISC forwarding.		
netbios-forward	Enable/disable NETBIOS forwarding.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable NETBIOS forwarding.		
	<i>enable</i>	Enable NETBIOS forwarding.		
netflow-sampler	Enable/disable NetFlow on this interface and set the data that NetFlow collects (rx, tx, or both).	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable NetFlow protocol on this interface.		
	<i>tx</i>	Monitor transmitted traffic on this interface.		
	<i>rx</i>	Monitor received traffic on this interface.		
	<i>both</i>	Monitor transmitted/received traffic on this interface.		
np-qos-profile *	NP QoS profile ID.	integer	Minimum value: 0 Maximum value: 15	0
outbandwidth	Bandwidth limit for outgoing traffic.	integer	Minimum value: 0 Maximum value: 80000000 **	0
padt-retry-timeout	PPPoE Active Discovery Terminate (PADT) used to terminate sessions after an idle time.	integer	Minimum value: 0 Maximum value: 4294967295	1
password	PPPoE account's password.	password	Not Specified	
phy-mode *	DSL physical mode.	option	-	vdsl
	<b>Option</b>	<b>Description</b>		
	<i>vdsl</i>	VDSL.		

Parameter	Description	Type	Size	Default
ping-serv-status	PING server status.	integer	Minimum value: 0 Maximum value: 255	0
poe *	Enable/disable PoE status.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable PoE status.		
	<i>disable</i>	Disable PoE status.		
polling-interval	sFlow polling interval in seconds.	integer	Minimum value: 1 Maximum value: 255	20
pppoe-unnumbered-negotiate	Enable/disable PPPoE unnumbered negotiation.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable IP address negotiating for unnumbered.		
	<i>disable</i>	Disable IP address negotiating for unnumbered.		
pptp-auth-type	PPTP authentication type.	option	-	auto
	<b>Option</b>	<b>Description</b>		
	<i>auto</i>	Automatically choose authentication.		
	<i>pap</i>	PAP authentication.		
	<i>chap</i>	CHAP authentication.		
	<i>mschapv1</i>	MS-CHAPv1 authentication.		
	<i>mschapv2</i>	MS-CHAPv2 authentication.		
pptp-client	Enable/disable PPTP client.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable PPTP client.		
	<i>disable</i>	Disable PPTP client.		
pptp-password	PPTP password.	password	Not Specified	
pptp-server-ip	PPTP server IP address.	ipv4-address	Not Specified	0.0.0.0

Parameter	Description	Type	Size	Default										
pptp-timeout	Idle timer in minutes (0 for disabled).	integer	Minimum value: 0 Maximum value: 65535	0										
pptp-user	PPTP user name.	string	Maximum length: 64											
preserve-session-route	Enable/disable preservation of session route when dirty.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable preservation of session route when dirty.</td></tr><tr><td>disable</td><td>Disable preservation of session route when dirty.</td></tr></table>	Option	Description	enable	Enable preservation of session route when dirty.	disable	Disable preservation of session route when dirty.							
Option	Description													
enable	Enable preservation of session route when dirty.													
disable	Disable preservation of session route when dirty.													
priority	Priority of learned routes.	integer	Minimum value: 1 Maximum value: 65535	1										
priority-override	Enable/disable fail back to higher priority port once recovered.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable fail back to higher priority port once recovered.</td></tr><tr><td>disable</td><td>Disable fail back to higher priority port once recovered.</td></tr></table>	Option	Description	enable	Enable fail back to higher priority port once recovered.	disable	Disable fail back to higher priority port once recovered.							
Option	Description													
enable	Enable fail back to higher priority port once recovered.													
disable	Disable fail back to higher priority port once recovered.													
proxy-captive-portal	Enable/disable proxy captive portal on this interface.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable proxy captive portal on this interface.</td></tr><tr><td>disable</td><td>Disable proxy captive portal on this interface.</td></tr></table>	Option	Description	enable	Enable proxy captive portal on this interface.	disable	Disable proxy captive portal on this interface.							
Option	Description													
enable	Enable proxy captive portal on this interface.													
disable	Disable proxy captive portal on this interface.													
pvc-atm-qos *	SFP-DSL ADSL Fallback PVC ATM QoS.	option	-	cbr										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>cbr</td><td>ATM QoS CBR.</td></tr><tr><td>rt-vbr</td><td>ATM QoS rt-VBR.</td></tr><tr><td>nrt-vbr</td><td>ATM QoS nrt-VBR.</td></tr><tr><td>cbr</td><td>ATM QoS CCBR.</td></tr></table>	Option	Description	cbr	ATM QoS CBR.	rt-vbr	ATM QoS rt-VBR.	nrt-vbr	ATM QoS nrt-VBR.	cbr	ATM QoS CCBR.			
Option	Description													
cbr	ATM QoS CBR.													
rt-vbr	ATM QoS rt-VBR.													
nrt-vbr	ATM QoS nrt-VBR.													
cbr	ATM QoS CCBR.													

Parameter	Description	Type	Size	Default								
pvc-chan *	SFP-DSL ADSL Fallback PVC Channel.	integer	Minimum value: 0 Maximum value: 7	0								
pvc-crc *	SFP-DSL ADSL Fallback PVC CRC Option: bit0: sar LLC preserve, bit1: ream LLC preserve, bit2: ream VC-MUX has crc.	integer	Minimum value: 0 Maximum value: 7	2								
pvc-pcr *	SFP-DSL ADSL Fallback PVC Packet Cell Rate in cells.	integer	Minimum value: 0 Maximum value: 5500	0								
pvc-scr *	SFP-DSL ADSL Fallback PVC Sustainable Cell Rate in cells.	integer	Minimum value: 0 Maximum value: 5500	0								
pvc-vlan-id *	SFP-DSL ADSL Fallback PVC VLAN ID.	integer	Minimum value: 1 Maximum value: 4094	7								
pvc-vlan-rx-id *	SFP-DSL ADSL Fallback PVC VLANID RX.	integer	Minimum value: 1 Maximum value: 4094	7								
pvc-vlan-rx-op *	SFP-DSL ADSL Fallback PVC VLAN RX op.	option	-	pass-through								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>pass-through</i></td><td>PVC VLAN Tag Passthrough.</td></tr><tr><td><i>replace</i></td><td>PVC VLAN Tag Replace.</td></tr><tr><td><i>remove</i></td><td>PVC VLAN Tag Remove.</td></tr></table>				Option	Description	<i>pass-through</i>	PVC VLAN Tag Passthrough.	<i>replace</i>	PVC VLAN Tag Replace.	<i>remove</i>	PVC VLAN Tag Remove.
Option	Description											
<i>pass-through</i>	PVC VLAN Tag Passthrough.											
<i>replace</i>	PVC VLAN Tag Replace.											
<i>remove</i>	PVC VLAN Tag Remove.											
pvc-vlan-tx-id *	SFP-DSL ADSL Fallback PVC VLAN ID TX.	integer	Minimum value: 1 Maximum value: 4094	7								
pvc-vlan-tx-op *	SFP-DSL ADSL Fallback PVC VLAN TX op.	option	-	remove								

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>pass-through</i>	PVC VLAN Tag Passthrough.		
	<i>replace</i>	PVC VLAN Tag Replace.		
	<i>remove</i>	PVC VLAN Tag Remove.		
reachable-time	IPv4 reachable time in milliseconds.	integer	Minimum value: 30000 Maximum value: 3600000	30000
redundant-interface	Redundant interface.	string	Maximum length: 15	
remote-ip	Remote IP address of tunnel.	ipv4-classnet-host	Not Specified	0.0.0.0 0.0.0.0
replacemsg-override-group	Replacement message override group.	string	Maximum length: 35	
retransmission *	Enable/disable DSL retransmission.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable retransmission.		
	<i>enable</i>	Enable retransmission.		
ring-rx *	RX ring size.	integer	Minimum value: 0 Maximum value: 4294967295	0
ring-tx *	TX ring size.	integer	Minimum value: 0 Maximum value: 4294967295	0
role	Interface role.	option	-	undefined
	<b>Option</b>	<b>Description</b>		
	<i>lan</i>	Connected to local network of endpoints.		
	<i>wan</i>	Connected to Internet.		



Parameter	Description	Type	Size	Default										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>dmz</i></td><td>Connected to server zone.</td></tr><tr><td><i>undefined</i></td><td>Interface has no specific role.</td></tr></table>	Option	Description	<i>dmz</i>	Connected to server zone.	<i>undefined</i>	Interface has no specific role.							
	Option	Description												
	<i>dmz</i>	Connected to server zone.												
<i>undefined</i>	Interface has no specific role.													
sample-direction	Data that NetFlow collects (rx, tx, or both).	option	-	both										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>tx</i></td><td>Monitor transmitted traffic on this interface.</td></tr><tr><td><i>rx</i></td><td>Monitor received traffic on this interface.</td></tr><tr><td><i>both</i></td><td>Monitor transmitted/received traffic on this interface.</td></tr></table>	Option	Description	<i>tx</i>	Monitor transmitted traffic on this interface.	<i>rx</i>	Monitor received traffic on this interface.	<i>both</i>	Monitor transmitted/received traffic on this interface.					
	Option	Description												
	<i>tx</i>	Monitor transmitted traffic on this interface.												
	<i>rx</i>	Monitor received traffic on this interface.												
<i>both</i>	Monitor transmitted/received traffic on this interface.													
sample-rate	sFlow sample rate.	integer	Minimum value: 10 Maximum value: 99999	2000										
secondary-IP	Enable/disable adding a secondary IP to this interface.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable secondary IP.</td></tr><tr><td><i>disable</i></td><td>Disable secondary IP.</td></tr></table>	Option	Description	<i>enable</i>	Enable secondary IP.	<i>disable</i>	Disable secondary IP.							
	Option	Description												
	<i>enable</i>	Enable secondary IP.												
<i>disable</i>	Disable secondary IP.													
security-8021x-dynamic-vlan-id *	VLAN ID for virtual switch.	integer	Minimum value: 0 Maximum value: 4094	0										
security-8021x-master *	802.1X master virtual-switch.	string	Maximum length: 15											
security-8021x-mode *	802.1X mode.	option	-	default										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>802.1X default mode.</td></tr><tr><td><i>dynamic-vlan</i></td><td>802.1X dynamic VLAN (master) mode.</td></tr><tr><td><i>fallback</i></td><td>802.1X fallback (master) mode.</td></tr><tr><td><i>slave</i></td><td>802.1X slave mode.</td></tr></table>	Option	Description	<i>default</i>	802.1X default mode.	<i>dynamic-vlan</i>	802.1X dynamic VLAN (master) mode.	<i>fallback</i>	802.1X fallback (master) mode.	<i>slave</i>	802.1X slave mode.			
	Option	Description												
	<i>default</i>	802.1X default mode.												
	<i>dynamic-vlan</i>	802.1X dynamic VLAN (master) mode.												
	<i>fallback</i>	802.1X fallback (master) mode.												
<i>slave</i>	802.1X slave mode.													

Parameter	Description	Type	Size	Default								
security-exempt-list	Name of security-exempt-list.	string	Maximum length: 35									
security-external-logout	URL of external authentication logout server.	string	Maximum length: 127									
security-external-web	URL of external authentication web server.	var-string	Maximum length: 1023									
security-groups <name>	User groups that can authenticate with the captive portal.  Names of user groups that can authenticate with the captive portal.	string	Maximum length: 79									
security-mac-auth-bypass	Enable/disable MAC authentication bypass.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>mac-auth-only</td><td>Enable MAC authentication bypass without EAP.</td></tr><tr><td>enable</td><td>Enable MAC authentication bypass.</td></tr><tr><td>disable</td><td>Disable MAC authentication bypass.</td></tr></table>				Option	Description	mac-auth-only	Enable MAC authentication bypass without EAP.	enable	Enable MAC authentication bypass.	disable	Disable MAC authentication bypass.
Option	Description											
mac-auth-only	Enable MAC authentication bypass without EAP.											
enable	Enable MAC authentication bypass.											
disable	Disable MAC authentication bypass.											
security-mode	Turn on captive portal authentication for this interface.	option	-	none								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>none</td><td>No security option.</td></tr><tr><td>captive-portal</td><td>Captive portal authentication.</td></tr><tr><td>802.1X</td><td>802.1X port-based authentication.</td></tr></table>				Option	Description	none	No security option.	captive-portal	Captive portal authentication.	802.1X	802.1X port-based authentication.
Option	Description											
none	No security option.											
captive-portal	Captive portal authentication.											
802.1X	802.1X port-based authentication.											
security-redirect-url	URL redirection after disclaimer/authentication.	var-string	Maximum length: 1023									
service-name	PPPoE service name.	string	Maximum length: 63									
sflow-sampler	Enable/disable sFlow on this interface.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable sFlow protocol on this interface.</td></tr><tr><td>disable</td><td>Disable sFlow protocol on this interface.</td></tr></table>				Option	Description	enable	Enable sFlow protocol on this interface.	disable	Disable sFlow protocol on this interface.		
Option	Description											
enable	Enable sFlow protocol on this interface.											
disable	Disable sFlow protocol on this interface.											
sfp-dsl *	Enable/disable SFP DSL.	option	-	disable								

Parameter	Description	Type	Size	Default																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable SFP DSL.</td></tr><tr><td><i>enable</i></td><td>Enable SFP DSL.</td></tr></table>	Option	Description	<i>disable</i>	Disable SFP DSL.	<i>enable</i>	Enable SFP DSL.													
	Option	Description																		
	<i>disable</i>	Disable SFP DSL.																		
<i>enable</i>	Enable SFP DSL.																			
sfp-dsl-adsl-fallback *	Enable/disable SFP DSL ADSL fallback.	option	-	disable																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable SFP DSL ADSL fallback.</td></tr><tr><td><i>enable</i></td><td>Enable SFP DSL ADSL fallback.</td></tr></table>	Option	Description	<i>disable</i>	Disable SFP DSL ADSL fallback.	<i>enable</i>	Enable SFP DSL ADSL fallback.													
	Option	Description																		
	<i>disable</i>	Disable SFP DSL ADSL fallback.																		
<i>enable</i>	Enable SFP DSL ADSL fallback.																			
sfp-dsl-autodetect *	Enable/disable SFP DSL MAC address autodetect.	option	-	enable																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable SFP DSL MAC address autodetect.</td></tr><tr><td><i>enable</i></td><td>Enable SFP DSL MAC address autodetect.</td></tr></table>	Option	Description	<i>disable</i>	Disable SFP DSL MAC address autodetect.	<i>enable</i>	Enable SFP DSL MAC address autodetect.													
	Option	Description																		
	<i>disable</i>	Disable SFP DSL MAC address autodetect.																		
<i>enable</i>	Enable SFP DSL MAC address autodetect.																			
sfp-dsl-mac *	SFP DSL MAC address.	mac-address	Not Specified	00:00:00:00:00:00																
snmp-index	Permanent SNMP Index of the interface.	integer	Minimum value: 1 Maximum value: 2147483647	0																
speed	Interface speed. The default setting and the options available depend on the interface hardware.	option	-	auto																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto</i></td><td>Automatically adjust speed.</td></tr><tr><td><i>10full</i></td><td>10M full-duplex.</td></tr><tr><td><i>10half</i></td><td>10M half-duplex.</td></tr><tr><td><i>100full</i></td><td>100M full-duplex.</td></tr><tr><td><i>100half</i></td><td>100M half-duplex.</td></tr><tr><td><i>1000full</i></td><td>1000M full-duplex.</td></tr><tr><td><i>1000auto</i></td><td>1000M auto adjust.</td></tr></table>	Option	Description	<i>auto</i>	Automatically adjust speed.	<i>10full</i>	10M full-duplex.	<i>10half</i>	10M half-duplex.	<i>100full</i>	100M full-duplex.	<i>100half</i>	100M half-duplex.	<i>1000full</i>	1000M full-duplex.	<i>1000auto</i>	1000M auto adjust.			
	Option	Description																		
	<i>auto</i>	Automatically adjust speed.																		
	<i>10full</i>	10M full-duplex.																		
	<i>10half</i>	10M half-duplex.																		
	<i>100full</i>	100M full-duplex.																		
	<i>100half</i>	100M half-duplex.																		
	<i>1000full</i>	1000M full-duplex.																		
<i>1000auto</i>	1000M auto adjust.																			

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>10000full</i></td><td>10G full-duplex.</td></tr><tr><td><i>10000auto</i></td><td>10G auto.</td></tr></table>	Option	Description	<i>10000full</i>	10G full-duplex.	<i>10000auto</i>	10G auto.					
	Option	Description										
	<i>10000full</i>	10G full-duplex.										
<i>10000auto</i>	10G auto.											
spillover-threshold	Egress Spillover threshold , 0 means unlimited.	integer	Minimum value: 0 Maximum value: 16776000	0								
src-check	Enable/disable source IP check.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable source IP check.</td></tr><tr><td><i>disable</i></td><td>Disable source IP check.</td></tr></table>	Option	Description	<i>enable</i>	Enable source IP check.	<i>disable</i>	Disable source IP check.					
	Option	Description										
	<i>enable</i>	Enable source IP check.										
<i>disable</i>	Disable source IP check.											
status	Bring the interface up or shut the interface down.	option	-	up								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>up</i></td><td>Bring the interface up.</td></tr><tr><td><i>down</i></td><td>Shut the interface down.</td></tr></table>	Option	Description	<i>up</i>	Bring the interface up.	<i>down</i>	Shut the interface down.					
	Option	Description										
	<i>up</i>	Bring the interface up.										
<i>down</i>	Shut the interface down.											
stp *	Enable/disable STP.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable STP.</td></tr><tr><td><i>enable</i></td><td>Enable STP.</td></tr></table>	Option	Description	<i>disable</i>	Disable STP.	<i>enable</i>	Enable STP.					
	Option	Description										
	<i>disable</i>	Disable STP.										
<i>enable</i>	Enable STP.											
stp-ha-secondary *	Control STP behaviour on HA secondary.	option	-	priority-adjust								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable STP negotiation on HA secondary.</td></tr><tr><td><i>enable</i></td><td>Enable STP negotiation on HA secondary.</td></tr><tr><td><i>priority-adjust</i></td><td>Enable STP negotiation on HA secondary and make priority lower than HA primary.</td></tr></table>	Option	Description	<i>disable</i>	Disable STP negotiation on HA secondary.	<i>enable</i>	Enable STP negotiation on HA secondary.	<i>priority-adjust</i>	Enable STP negotiation on HA secondary and make priority lower than HA primary.			
	Option	Description										
	<i>disable</i>	Disable STP negotiation on HA secondary.										
	<i>enable</i>	Enable STP negotiation on HA secondary.										
<i>priority-adjust</i>	Enable STP negotiation on HA secondary and make priority lower than HA primary.											
stpforward	Enable/disable STP forwarding.	option	-	disable								

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable STP forwarding.</td></tr><tr><td><i>disable</i></td><td>Disable STP forwarding.</td></tr></table>	Option	Description	<i>enable</i>	Enable STP forwarding.	<i>disable</i>	Disable STP forwarding.					
	Option	Description										
	<i>enable</i>	Enable STP forwarding.										
<i>disable</i>	Disable STP forwarding.											
stpforward-mode	Configure STP forwarding mode.	option	-	rpl-all-ext-id								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>rpl-all-ext-id</i></td><td>Replace all extension IDs (root, bridge).</td></tr><tr><td><i>rpl-bridge-ext-id</i></td><td>Replace the bridge extension ID only.</td></tr><tr><td><i>rpl-nothing</i></td><td>Replace nothing.</td></tr></table>	Option	Description	<i>rpl-all-ext-id</i>	Replace all extension IDs (root, bridge).	<i>rpl-bridge-ext-id</i>	Replace the bridge extension ID only.	<i>rpl-nothing</i>	Replace nothing.			
	Option	Description										
	<i>rpl-all-ext-id</i>	Replace all extension IDs (root, bridge).										
	<i>rpl-bridge-ext-id</i>	Replace the bridge extension ID only.										
<i>rpl-nothing</i>	Replace nothing.											
subst	Enable to always send packets from this interface to a destination MAC address.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Send packets from this interface.</td></tr><tr><td><i>disable</i></td><td>Do not send packets from this interface.</td></tr></table>	Option	Description	<i>enable</i>	Send packets from this interface.	<i>disable</i>	Do not send packets from this interface.					
	Option	Description										
	<i>enable</i>	Send packets from this interface.										
<i>disable</i>	Do not send packets from this interface.											
substitute-dst-mac	Destination MAC address that all packets are sent to from this interface.	mac-address	Not Specified	00:00:00:00:00:00								
sw-algorithm *	Frame distribution algorithm for switch.	option	-	eh								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>l2</i></td><td>Use layer 2 address for distribution.</td></tr><tr><td><i>l3</i></td><td>Use layer 3 address for distribution.</td></tr><tr><td><i>eh</i></td><td>Use enhanced hashing for distribution.</td></tr></table>	Option	Description	<i>l2</i>	Use layer 2 address for distribution.	<i>l3</i>	Use layer 3 address for distribution.	<i>eh</i>	Use enhanced hashing for distribution.			
	Option	Description										
	<i>l2</i>	Use layer 2 address for distribution.										
	<i>l3</i>	Use layer 3 address for distribution.										
<i>eh</i>	Use enhanced hashing for distribution.											
swc-first-create *	Initial create for switch-controller VLANs.	integer	Minimum value: 0 Maximum value: 4294967295	0								
swc-vlan *	Creation status for switch-controller VLANs.	integer	Minimum value: 0 Maximum value: 4294967295	0								
switch	Contained in switch.	string	Maximum length: 15									

Parameter	Description	Type	Size	Default						
switch-controller-access-vlan *	Block FortiSwitch port-to-port traffic.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Block FortiSwitch port-to-port traffic on the VLAN, only permitting traffic to and from the FortiGate.</td></tr><tr><td><i>disable</i></td><td>Allow normal VLAN traffic.</td></tr></table>	Option	Description	<i>enable</i>	Block FortiSwitch port-to-port traffic on the VLAN, only permitting traffic to and from the FortiGate.	<i>disable</i>	Allow normal VLAN traffic.			
Option	Description									
<i>enable</i>	Block FortiSwitch port-to-port traffic on the VLAN, only permitting traffic to and from the FortiGate.									
<i>disable</i>	Allow normal VLAN traffic.									
switch-controller-arp-inspection *	Enable/disable FortiSwitch ARP inspection.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable ARP inspection for FortiSwitch devices.</td></tr><tr><td><i>disable</i></td><td>Disable ARP inspection for FortiSwitch devices.</td></tr></table>	Option	Description	<i>enable</i>	Enable ARP inspection for FortiSwitch devices.	<i>disable</i>	Disable ARP inspection for FortiSwitch devices.			
Option	Description									
<i>enable</i>	Enable ARP inspection for FortiSwitch devices.									
<i>disable</i>	Disable ARP inspection for FortiSwitch devices.									
switch-controller-dhcp-snooping *	Switch controller DHCP snooping.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable DHCP snooping for FortiSwitch devices.</td></tr><tr><td><i>disable</i></td><td>Disable DHCP snooping for FortiSwitch devices.</td></tr></table>	Option	Description	<i>enable</i>	Enable DHCP snooping for FortiSwitch devices.	<i>disable</i>	Disable DHCP snooping for FortiSwitch devices.			
Option	Description									
<i>enable</i>	Enable DHCP snooping for FortiSwitch devices.									
<i>disable</i>	Disable DHCP snooping for FortiSwitch devices.									
switch-controller-dhcp-snooping-option82 *	Switch controller DHCP snooping option82.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable DHCP snooping insert option82 for FortiSwitch devices.</td></tr><tr><td><i>disable</i></td><td>Disable DHCP snooping insert option82 for FortiSwitch devices.</td></tr></table>	Option	Description	<i>enable</i>	Enable DHCP snooping insert option82 for FortiSwitch devices.	<i>disable</i>	Disable DHCP snooping insert option82 for FortiSwitch devices.			
Option	Description									
<i>enable</i>	Enable DHCP snooping insert option82 for FortiSwitch devices.									
<i>disable</i>	Disable DHCP snooping insert option82 for FortiSwitch devices.									
switch-controller-dhcp-snooping-verify-mac *	Switch controller DHCP snooping verify MAC.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable DHCP snooping verify source MAC for FortiSwitch devices.</td></tr><tr><td><i>disable</i></td><td>Disable DHCP snooping verify source MAC for FortiSwitch devices.</td></tr></table>	Option	Description	<i>enable</i>	Enable DHCP snooping verify source MAC for FortiSwitch devices.	<i>disable</i>	Disable DHCP snooping verify source MAC for FortiSwitch devices.			
Option	Description									
<i>enable</i>	Enable DHCP snooping verify source MAC for FortiSwitch devices.									
<i>disable</i>	Disable DHCP snooping verify source MAC for FortiSwitch devices.									
switch-controller-dynamic *	Integrated FortiLink settings for managed FortiSwitch.	string	Maximum length: 35							
switch-controller-feature *	Interface's purpose when assigning traffic (read only).	option	-	none						

Parameter	Description	Type	Size	Default																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>VLAN for generic purpose.</td></tr><tr><td><i>default-vlan</i></td><td>Default VLAN (native) assigned to all switch ports upon discovery.</td></tr><tr><td><i>quarantine</i></td><td>VLAN for quarantined traffic.</td></tr><tr><td><i>rspan</i></td><td>VLAN for RSPAN/ERSPAN mirrored traffic.</td></tr><tr><td><i>voice</i></td><td>VLAN dedicated for voice devices.</td></tr><tr><td><i>video</i></td><td>VLAN dedicated for camera devices.</td></tr><tr><td><i>nac</i></td><td>VLAN dedicated for NAC onboarding devices.</td></tr><tr><td><i>nac-segment</i></td><td>VLAN dedicated for NAC segment devices.</td></tr></table>	Option	Description	<i>none</i>	VLAN for generic purpose.	<i>default-vlan</i>	Default VLAN (native) assigned to all switch ports upon discovery.	<i>quarantine</i>	VLAN for quarantined traffic.	<i>rspan</i>	VLAN for RSPAN/ERSPAN mirrored traffic.	<i>voice</i>	VLAN dedicated for voice devices.	<i>video</i>	VLAN dedicated for camera devices.	<i>nac</i>	VLAN dedicated for NAC onboarding devices.	<i>nac-segment</i>	VLAN dedicated for NAC segment devices.			
	Option	Description																				
	<i>none</i>	VLAN for generic purpose.																				
	<i>default-vlan</i>	Default VLAN (native) assigned to all switch ports upon discovery.																				
	<i>quarantine</i>	VLAN for quarantined traffic.																				
	<i>rspan</i>	VLAN for RSPAN/ERSPAN mirrored traffic.																				
	<i>voice</i>	VLAN dedicated for voice devices.																				
	<i>video</i>	VLAN dedicated for camera devices.																				
	<i>nac</i>	VLAN dedicated for NAC onboarding devices.																				
<i>nac-segment</i>	VLAN dedicated for NAC segment devices.																					
switch-controller-igmp-snooping *	Switch controller IGMP snooping.	option	-	disable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable IGMP snooping.</td></tr><tr><td><i>disable</i></td><td>Disable IGMP snooping.</td></tr></table>	Option	Description	<i>enable</i>	Enable IGMP snooping.	<i>disable</i>	Disable IGMP snooping.															
	Option	Description																				
	<i>enable</i>	Enable IGMP snooping.																				
<i>disable</i>	Disable IGMP snooping.																					
switch-controller-igmp-snooping-fast-leave *	Switch controller IGMP snooping fast-leave.	option	-	disable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable IGMP snooping fast-leave.</td></tr><tr><td><i>disable</i></td><td>Disable IGMP snooping fast-leave.</td></tr></table>	Option	Description	<i>enable</i>	Enable IGMP snooping fast-leave.	<i>disable</i>	Disable IGMP snooping fast-leave.															
	Option	Description																				
	<i>enable</i>	Enable IGMP snooping fast-leave.																				
<i>disable</i>	Disable IGMP snooping fast-leave.																					
switch-controller-igmp-snooping-proxy *	Switch controller IGMP snooping proxy.	option	-	disable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable IGMP snooping proxy.</td></tr><tr><td><i>disable</i></td><td>Disable IGMP snooping proxy.</td></tr></table>	Option	Description	<i>enable</i>	Enable IGMP snooping proxy.	<i>disable</i>	Disable IGMP snooping proxy.															
	Option	Description																				
	<i>enable</i>	Enable IGMP snooping proxy.																				
<i>disable</i>	Disable IGMP snooping proxy.																					
switch-controller-iot-scanning *	Enable/disable managed FortiSwitch IoT scanning.	option	-	disable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable IoT scanning for managed FortiSwitch devices.</td></tr><tr><td><i>disable</i></td><td>Disable IoT scanning for managed FortiSwitch devices.</td></tr></table>	Option	Description	<i>enable</i>	Enable IoT scanning for managed FortiSwitch devices.	<i>disable</i>	Disable IoT scanning for managed FortiSwitch devices.															
	Option	Description																				
	<i>enable</i>	Enable IoT scanning for managed FortiSwitch devices.																				
<i>disable</i>	Disable IoT scanning for managed FortiSwitch devices.																					

Parameter	Description	Type	Size	Default						
switch-controller-learning-limit *	Limit the number of dynamic MAC addresses on this VLAN.	integer	Minimum value: 0 Maximum value: 128	0						
switch-controller-mgmt-vlan *	VLAN to use for FortiLink management purposes.	integer	Minimum value: 1 Maximum value: 4094	4094						
switch-controller-nac *	Integrated FortiLink settings for managed FortiSwitch.	string	Maximum length: 35							
switch-controller-rspan-mode *	Stop Layer2 MAC learning and interception of BPDUs and other packets on this interface.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable RSPAN passthrough mode on this VLAN interface.</td></tr><tr><td>enable</td><td>Enable RSPAN passthrough mode on this VLAN interface.</td></tr></table>				Option	Description	disable	Disable RSPAN passthrough mode on this VLAN interface.	enable	Enable RSPAN passthrough mode on this VLAN interface.
Option	Description									
disable	Disable RSPAN passthrough mode on this VLAN interface.									
enable	Enable RSPAN passthrough mode on this VLAN interface.									
switch-controller-source-ip *	Source IP address used in FortiLink over L3 connections.	option	-	outbound						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>outbound</td><td>Source IP address is that of the outbound interface.</td></tr><tr><td>fixed</td><td>Source IP address is that of the FortiLink interface.</td></tr></table>				Option	Description	outbound	Source IP address is that of the outbound interface.	fixed	Source IP address is that of the FortiLink interface.
Option	Description									
outbound	Source IP address is that of the outbound interface.									
fixed	Source IP address is that of the FortiLink interface.									
switch-controller-traffic-policy *	Switch controller traffic policy for the VLAN.	string	Maximum length: 63							
system-id	Define a system ID for the aggregate interface.	mac-address	Not Specified	00:00:00:00:00:00						
system-id-type	Method in which system ID is generated.	option	-	auto						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>auto</td><td>Use the MAC address of the first member.</td></tr><tr><td>user</td><td>User-defined system ID.</td></tr></table>				Option	Description	auto	Use the MAC address of the first member.	user	User-defined system ID.
Option	Description									
auto	Use the MAC address of the first member.									
user	User-defined system ID.									
tc-mode *	DSL transfer mode.	option	-	ptm						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ptm</td><td>Packet transfer mode.</td></tr></table>				Option	Description	ptm	Packet transfer mode.		
Option	Description									
ptm	Packet transfer mode.									



Parameter	Description	Type	Size	Default
tcp-mss	TCP maximum segment size. 0 means do not change segment size.	integer	Minimum value: 48 Maximum value: 65535	0
trunk *	Enable/disable VLAN trunk.	option	-	disable
	<div>OptionDescription</div>			
	enable	Enable VLAN trunk on this interface.		
	disable	Disable VLAN trunk on this interface.		
trust-ip-1	Trusted host for dedicated management traffic (0.0.0.0/24 for all hosts).	ipv4-classnet-any	Not Specified	0.0.0.0 0.0.0.0
trust-ip-2	Trusted host for dedicated management traffic (0.0.0.0/24 for all hosts).	ipv4-classnet-any	Not Specified	0.0.0.0 0.0.0.0
trust-ip-3	Trusted host for dedicated management traffic (0.0.0.0/24 for all hosts).	ipv4-classnet-any	Not Specified	0.0.0.0 0.0.0.0
trust-ip6-1	Trusted IPv6 host for dedicated management traffic (::/0 for all hosts).	ipv6-prefix	Not Specified	::/0
trust-ip6-2	Trusted IPv6 host for dedicated management traffic (::/0 for all hosts).	ipv6-prefix	Not Specified	::/0
trust-ip6-3	Trusted IPv6 host for dedicated management traffic (::/0 for all hosts).	ipv6-prefix	Not Specified	::/0
type	Interface type.	option	-	vlan
	<div>OptionDescription</div>			
	physical	Physical interface.		
	vlan	VLAN interface.		
	aggregate	Aggregate interface.		
	redundant	Redundant interface.		
	tunnel	Tunnel interface.		
	vdom-link	VDOM link interface.		
	loopback	Loopback interface.		
	switch	Software switch interface.		

Parameter	Description	Type	Size	Default																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>vap-switch</i></td><td>VAP interface.</td></tr><tr><td><i>wl-mesh</i></td><td>WLAN mesh interface.</td></tr><tr><td><i>fext-wan</i></td><td>FortiExtender interface.</td></tr><tr><td><i>vxlan</i></td><td>VXLAN interface.</td></tr><tr><td><i>geneve</i></td><td>GENEVE interface.</td></tr><tr><td><i>hdlc</i></td><td>T1/E1 interface.</td></tr><tr><td><i>switch-vlan</i></td><td>Switch VLAN interface.</td></tr><tr><td><i>emac-vlan</i></td><td>EMAC VLAN interface.</td></tr><tr><td><i>ssl</i></td><td>SSL VPN client interface.</td></tr><tr><td><i>lan-extension</i></td><td>LAN extension interface.</td></tr></table>				Option	Description	<i>vap-switch</i>	VAP interface.	<i>wl-mesh</i>	WLAN mesh interface.	<i>fext-wan</i>	FortiExtender interface.	<i>vxlan</i>	VXLAN interface.	<i>geneve</i>	GENEVE interface.	<i>hdlc</i>	T1/E1 interface.	<i>switch-vlan</i>	Switch VLAN interface.	<i>emac-vlan</i>	EMAC VLAN interface.	<i>ssl</i>	SSL VPN client interface.	<i>lan-extension</i>	LAN extension interface.
	Option	Description																								
	<i>vap-switch</i>	VAP interface.																								
	<i>wl-mesh</i>	WLAN mesh interface.																								
	<i>fext-wan</i>	FortiExtender interface.																								
	<i>vxlan</i>	VXLAN interface.																								
	<i>geneve</i>	GENEVE interface.																								
	<i>hdlc</i>	T1/E1 interface.																								
	<i>switch-vlan</i>	Switch VLAN interface.																								
	<i>emac-vlan</i>	EMAC VLAN interface.																								
	<i>ssl</i>	SSL VPN client interface.																								
<i>lan-extension</i>	LAN extension interface.																									
username	Username of the PPPoE account, provided by your ISP.	string	Maximum length: 64																							
vci *	Virtual Channel ID	integer	Minimum value: 0 Maximum value: 65535	35																						
vdom	Interface is in this virtual domain (VDOM).	string	Maximum length: 31																							
vectoring *	Enable/disable DSL vectoring.	option	-	enable																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable vectoring.</td></tr><tr><td><i>enable</i></td><td>Enable vectoring.</td></tr></table>				Option	Description	<i>disable</i>	Disable vectoring.	<i>enable</i>	Enable vectoring.																
	Option	Description																								
	<i>disable</i>	Disable vectoring.																								
<i>enable</i>	Enable vectoring.																									
vindex *	Switch control interface VLAN ID.	integer	Minimum value: 0 Maximum value: 65535	0																						
vlan-protocol	Ethernet protocol of VLAN.	option	-	8021q																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>8021q</i></td><td>IEEE 802.1Q.</td></tr><tr><td><i>8021ad</i></td><td>IEEE 802.1AD.</td></tr></table>				Option	Description	<i>8021q</i>	IEEE 802.1Q.	<i>8021ad</i>	IEEE 802.1AD.																
	Option	Description																								
	<i>8021q</i>	IEEE 802.1Q.																								
<i>8021ad</i>	IEEE 802.1AD.																									

Parameter	Description	Type	Size	Default
vlanforward	Enable/disable traffic forwarding between VLANs on this interface.	option	-	disable
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Enable traffic forwarding.		
	<i>disable</i>	Disable traffic forwarding.		
vlanid	VLAN ID.	integer	Minimum value: 1 Maximum value: 4094	0
vpi *	Virtual Path ID.	integer	Minimum value: 0 Maximum value: 255	0
vrf	Virtual Routing Forwarding ID.	integer	Minimum value: 0 Maximum value: 31	0
vrrp-virtual-mac	Enable/disable use of virtual MAC for VRRP.	option	-	disable
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Enable use of virtual MAC for VRRP.		
	<i>disable</i>	Disable use of virtual MAC for VRRP.		
wccp	Enable/disable WCCP on this interface. Used for encapsulated WCCP communication between WCCP clients and servers.	option	-	disable
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Enable WCCP protocol on this interface.		
	<i>disable</i>	Disable WCCP protocol on this interface.		
weight	Default weight for static routes (if route has no weight configured).	integer	Minimum value: 0 Maximum value: 255	0
wifi-5g-threshold *	Minimal signal strength to be considered as a good 5G AP.	string	Maximum length: 7	-78

Parameter	Description	Type	Size	Default								
wifi-acl *	Access control for MAC addresses in the MAC list.	option	-	deny								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow.</td></tr><tr><td><i>deny</i></td><td>Deny.</td></tr></table>	Option	Description	<i>allow</i>	Allow.	<i>deny</i>	Deny.					
Option	Description											
<i>allow</i>	Allow.											
<i>deny</i>	Deny.											
wifi-ap-band *	How to select the AP to connect.	option	-	any								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>any</i></td><td>Connect to the best 2G or 5G AP.</td></tr><tr><td><i>5g-preferred</i></td><td>Connect to the 5G AP if a good 5G AP exists.</td></tr><tr><td><i>5g-only</i></td><td>Only connect to the 5G AP.</td></tr></table>	Option	Description	<i>any</i>	Connect to the best 2G or 5G AP.	<i>5g-preferred</i>	Connect to the 5G AP if a good 5G AP exists.	<i>5g-only</i>	Only connect to the 5G AP.			
Option	Description											
<i>any</i>	Connect to the best 2G or 5G AP.											
<i>5g-preferred</i>	Connect to the 5G AP if a good 5G AP exists.											
<i>5g-only</i>	Only connect to the 5G AP.											
wifi-auth *	WiFi authentication.	option	-	PSK								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>PSK</i></td><td>PSK.</td></tr><tr><td><i>radius</i></td><td>RADIUS.</td></tr><tr><td><i>usergroup</i></td><td>User group.</td></tr></table>	Option	Description	<i>PSK</i>	PSK.	<i>radius</i>	RADIUS.	<i>usergroup</i>	User group.			
Option	Description											
<i>PSK</i>	PSK.											
<i>radius</i>	RADIUS.											
<i>usergroup</i>	User group.											
wifi-auto-connect *	Enable/disable WiFi network auto connect.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable WiFi network auto connect.</td></tr><tr><td><i>disable</i></td><td>Disable WiFi network auto connect.</td></tr></table>	Option	Description	<i>enable</i>	Enable WiFi network auto connect.	<i>disable</i>	Disable WiFi network auto connect.					
Option	Description											
<i>enable</i>	Enable WiFi network auto connect.											
<i>disable</i>	Disable WiFi network auto connect.											
wifi-auto-save *	Enable/disable WiFi network automatic save.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable WiFi network automatic save.</td></tr><tr><td><i>disable</i></td><td>Disable WiFi network automatic save.</td></tr></table>	Option	Description	<i>enable</i>	Enable WiFi network automatic save.	<i>disable</i>	Disable WiFi network automatic save.					
Option	Description											
<i>enable</i>	Enable WiFi network automatic save.											
<i>disable</i>	Disable WiFi network automatic save.											
wifi-broadcast-ssid *	Enable/disable SSID broadcast in the beacon.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable SSID broadcast in the beacon.</td></tr></table>	Option	Description	<i>enable</i>	Enable SSID broadcast in the beacon.							
Option	Description											
<i>enable</i>	Enable SSID broadcast in the beacon.											

Parameter	Description	Type	Size	Default										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable SSID broadcast in the beacon.</td></tr></table>				Option	Description	<i>disable</i>	Disable SSID broadcast in the beacon.						
Option	Description													
<i>disable</i>	Disable SSID broadcast in the beacon.													
wifi-encrypt *	Data encryption.	option	-	AES										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>TKIP</i></td><td>TKIP.</td></tr><tr><td><i>AES</i></td><td>AES.</td></tr></table>				Option	Description	<i>TKIP</i>	TKIP.	<i>AES</i>	AES.				
Option	Description													
<i>TKIP</i>	TKIP.													
<i>AES</i>	AES.													
wifi-fragment-threshold *	WiFi fragment threshold.	integer	Minimum value: 800 Maximum value: 2346	2346										
wifi-key *	WiFi WEP Key.	password	Not Specified											
wifi-keyindex *	WEP key index.	integer	Minimum value: 1 Maximum value: 4	1										
wifi-mac-filter *	Enable/disable MAC filter status.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable MAC filter.</td></tr><tr><td><i>disable</i></td><td>Disable MAC filter.</td></tr></table>				Option	Description	<i>enable</i>	Enable MAC filter.	<i>disable</i>	Disable MAC filter.				
Option	Description													
<i>enable</i>	Enable MAC filter.													
<i>disable</i>	Disable MAC filter.													
wifi-passphrase *	WiFi pre-shared key for WPA.	password	Not Specified											
wifi-radius-server *	WiFi RADIUS server for WPA.	string	Maximum length: 35											
wifi-rts-threshold *	WiFi RTS threshold.	integer	Minimum value: 256 Maximum value: 2346	2346										
wifi-security *	Wireless access security of SSID.	option	-	wpa-personal										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>open</i></td><td>Open.</td></tr><tr><td><i>wep64</i></td><td>WEP64.</td></tr><tr><td><i>wep128</i></td><td>WEP128.</td></tr><tr><td><i>wpa-personal</i></td><td>WPA personal.</td></tr></table>				Option	Description	<i>open</i>	Open.	<i>wep64</i>	WEP64.	<i>wep128</i>	WEP128.	<i>wpa-personal</i>	WPA personal.
Option	Description													
<i>open</i>	Open.													
<i>wep64</i>	WEP64.													
<i>wep128</i>	WEP128.													
<i>wpa-personal</i>	WPA personal.													

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>wpa-enterprise</i>	WPA enterprise.		
	<i>wpa-only-personal</i>	WPA personal only.		
	<i>wpa-only-enterprise</i>	WPA enterprise only.		
	<i>wpa2-only-personal</i>	WPA2 personal only.		
	<i>wpa2-only-enterprise</i>	WPA2 enterprise only.		
wifi-ssid *	IEEE 802.11 Service Set Identifier.	string	Maximum length: 32	fortinet
wifi-usergroup *	WiFi user group for WPA.	string	Maximum length: 35	
wins-ip	WINS server IP.	ipv4-address	Not Specified	0.0.0.0

\* This parameter may not exist in some models.

\*\* Values may differ between models.

### config client-options

Parameter	Description	Type	Size	Default						
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0						
code	DHCP client option code.	integer	Minimum value: 0 Maximum value: 255	0						
type	DHCP client option type.	option	-	hex						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>hex</i></td><td>DHCP option in hex.</td></tr><tr><td><i>string</i></td><td>DHCP option in string.</td></tr></table>				Option	Description	<i>hex</i>	DHCP option in hex.	<i>string</i>	DHCP option in string.
Option	Description									
<i>hex</i>	DHCP option in hex.									
<i>string</i>	DHCP option in string.									

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>ip</i>	DHCP option in IP.		
	<i>fqdn</i>	DHCP option in domain search option format.		
value	DHCP client option value.	string	Maximum length: 312	
ip	DHCP option IPs.	user	Not Specified	

### config dhcp-snooping-server-list

Parameter	Description	Type	Size	Default
name	DHCP server name.	string	Maximum length: 35	default
server-ip	IP address for DHCP server.	ipv4-address	Not Specified	0.0.0.0

### config egress-queues

Parameter	Description	Type	Size	Default
cos0	CoS profile name for CoS 0.	string	Maximum length: 35	
cos1	CoS profile name for CoS 1.	string	Maximum length: 35	
cos2	CoS profile name for CoS 2.	string	Maximum length: 35	
cos3	CoS profile name for CoS 3.	string	Maximum length: 35	
cos4	CoS profile name for CoS 4.	string	Maximum length: 35	
cos5	CoS profile name for CoS 5.	string	Maximum length: 35	
cos6	CoS profile name for CoS 6.	string	Maximum length: 35	
cos7	CoS profile name for CoS 7.	string	Maximum length: 35	

## config ipv6

Parameter	Description	Type	Size	Default										
ip6-mode	Addressing mode (static, DHCP, delegated).	option	-	static										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>static</i></td><td>Static setting.</td></tr><tr><td><i>dhcp</i></td><td>DHCPv6 client mode.</td></tr><tr><td><i>pppoe</i></td><td>IPv6 over PPPoE mode.</td></tr><tr><td><i>delegated</i></td><td>IPv6 address with delegated prefix.</td></tr></table>	Option	Description	<i>static</i>	Static setting.	<i>dhcp</i>	DHCPv6 client mode.	<i>pppoe</i>	IPv6 over PPPoE mode.	<i>delegated</i>	IPv6 address with delegated prefix.			
Option	Description													
<i>static</i>	Static setting.													
<i>dhcp</i>	DHCPv6 client mode.													
<i>pppoe</i>	IPv6 over PPPoE mode.													
<i>delegated</i>	IPv6 address with delegated prefix.													
nd-mode	Neighbor discovery mode.	option	-	basic										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>basic</i></td><td>Do not support SEND.</td></tr><tr><td><i>SEND-compatible</i></td><td>Support SEND.</td></tr></table>	Option	Description	<i>basic</i>	Do not support SEND.	<i>SEND-compatible</i>	Support SEND.							
Option	Description													
<i>basic</i>	Do not support SEND.													
<i>SEND-compatible</i>	Support SEND.													
nd-cert	Neighbor discovery certificate.	string	Maximum length: 35											
nd-security-level	Neighbor discovery security level.	integer	Minimum value: 0 Maximum value: 7	0										
nd-timestamp-delta	Neighbor discovery timestamp delta value.	integer	Minimum value: 1 Maximum value: 3600	300										
nd-timestamp-fuzz	Neighbor discovery timestamp fuzz factor.	integer	Minimum value: 1 Maximum value: 60	1										
nd-cga-modifier	Neighbor discovery CGA modifier.	user	Not Specified											
ip6-dns-server-override	Enable/disable using the DNS server acquired by DHCP.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable using the DNS server acquired by DHCP.</td></tr><tr><td><i>disable</i></td><td>Disable using the DNS server acquired by DHCP.</td></tr></table>	Option	Description	<i>enable</i>	Enable using the DNS server acquired by DHCP.	<i>disable</i>	Disable using the DNS server acquired by DHCP.							
Option	Description													
<i>enable</i>	Enable using the DNS server acquired by DHCP.													
<i>disable</i>	Disable using the DNS server acquired by DHCP.													



Parameter	Description	Type	Size	Default																		
ip6-address	Primary IPv6 address prefix. Syntax: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/xxx.	ipv6-prefix	Not Specified	::/0																		
ip6-allowaccess	Allow management access to the interface.	option	-																			
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ping</i></td><td>PING access.</td></tr><tr><td><i>https</i></td><td>HTTPS access.</td></tr><tr><td><i>ssh</i></td><td>SSH access.</td></tr><tr><td><i>snmp</i></td><td>SNMP access.</td></tr><tr><td><i>http</i></td><td>HTTP access.</td></tr><tr><td><i>telnet</i></td><td>TELNET access.</td></tr><tr><td><i>fgfm</i></td><td>FortiManager access.</td></tr><tr><td><i>fabric</i></td><td>Fabric access.</td></tr></table>	Option	Description	<i>ping</i>	PING access.	<i>https</i>	HTTPS access.	<i>ssh</i>	SSH access.	<i>snmp</i>	SNMP access.	<i>http</i>	HTTP access.	<i>telnet</i>	TELNET access.	<i>fgfm</i>	FortiManager access.	<i>fabric</i>	Fabric access.			
Option	Description																					
<i>ping</i>	PING access.																					
<i>https</i>	HTTPS access.																					
<i>ssh</i>	SSH access.																					
<i>snmp</i>	SNMP access.																					
<i>http</i>	HTTP access.																					
<i>telnet</i>	TELNET access.																					
<i>fgfm</i>	FortiManager access.																					
<i>fabric</i>	Fabric access.																					
ip6-send-adv	Enable/disable sending advertisements about the interface.	option	-	disable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable sending advertisements about this interface.</td></tr><tr><td><i>disable</i></td><td>Disable sending advertisements about this interface.</td></tr></table>	Option	Description	<i>enable</i>	Enable sending advertisements about this interface.	<i>disable</i>	Disable sending advertisements about this interface.															
Option	Description																					
<i>enable</i>	Enable sending advertisements about this interface.																					
<i>disable</i>	Disable sending advertisements about this interface.																					
icmp6-send-redirect	Enable/disable sending of ICMPv6 redirects.	option	-	enable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable sending of ICMPv6 redirects.</td></tr><tr><td><i>disable</i></td><td>Disable sending of ICMPv6 redirects.</td></tr></table>	Option	Description	<i>enable</i>	Enable sending of ICMPv6 redirects.	<i>disable</i>	Disable sending of ICMPv6 redirects.															
Option	Description																					
<i>enable</i>	Enable sending of ICMPv6 redirects.																					
<i>disable</i>	Disable sending of ICMPv6 redirects.																					
ip6-manage-flag	Enable/disable the managed flag.	option	-	disable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable the managed IPv6 flag.</td></tr><tr><td><i>disable</i></td><td>Disable the managed IPv6 flag.</td></tr></table>	Option	Description	<i>enable</i>	Enable the managed IPv6 flag.	<i>disable</i>	Disable the managed IPv6 flag.															
Option	Description																					
<i>enable</i>	Enable the managed IPv6 flag.																					
<i>disable</i>	Disable the managed IPv6 flag.																					
ip6-other-flag	Enable/disable the other IPv6 flag.	option	-	disable																		

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable the other IPv6 flag.</td></tr><tr><td><i>disable</i></td><td>Disable the other IPv6 flag.</td></tr></table>	Option	Description	<i>enable</i>	Enable the other IPv6 flag.	<i>disable</i>	Disable the other IPv6 flag.			
	Option	Description								
	<i>enable</i>	Enable the other IPv6 flag.								
<i>disable</i>	Disable the other IPv6 flag.									
ip6-max-interval	IPv6 maximum interval (4 to 1800 sec).	integer	Minimum value: 4 Maximum value: 1800	600						
ip6-min-interval	IPv6 minimum interval (3 to 1350 sec).	integer	Minimum value: 3 Maximum value: 1350	198						
ip6-link-mtu	IPv6 link MTU.	integer	Minimum value: 1280 Maximum value: 16000	0						
ra-send-mtu	Enable/disable sending link MTU in RA packet.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable sending link MTU in RA packet.</td></tr><tr><td><i>disable</i></td><td>Disable sending link MTU in RA packet.</td></tr></table>	Option	Description	<i>enable</i>	Enable sending link MTU in RA packet.	<i>disable</i>	Disable sending link MTU in RA packet.			
	Option	Description								
	<i>enable</i>	Enable sending link MTU in RA packet.								
<i>disable</i>	Disable sending link MTU in RA packet.									
ip6-reachable-time	IPv6 reachable time (milliseconds; 0 means unspecified).	integer	Minimum value: 0 Maximum value: 3600000	0						
ip6-retrans-time	IPv6 retransmit time (milliseconds; 0 means unspecified).	integer	Minimum value: 0 Maximum value: 4294967295	0						
ip6-default-life	Default life (sec).	integer	Minimum value: 0 Maximum value: 9000	1800						
ip6-hop-limit	Hop limit (0 means unspecified).	integer	Minimum value: 0 Maximum value: 255	0						

Parameter	Description	Type	Size	Default
autoconf	Enable/disable address auto config.	option	-	disable
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Enable auto-configuration.		
	<i>disable</i>	Disable auto-configuration.		
unique-autoconf-addr	Enable/disable unique auto config address.	option	-	disable
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Enable unique auto-configuration address.		
	<i>disable</i>	Disable unique auto-configuration address.		
interface-identifier	IPv6 interface identifier.	ipv6-address	Not Specified	::
ip6-prefix-mode	Assigning a prefix from DHCP or RA.	option	-	dhcp6
	<b>Option</b> <b>Description</b>			
	<i>dhcp6</i>	Use delegated prefix from a DHCPv6 client to form a delegated IPv6 address.		
	<i>ra</i>	Use prefix from RA to form a delegated IPv6 address.		
ip6-upstream-interface	Interface name providing delegated information.	string	Maximum length: 15	
ip6-delegated-prefix-iaid	IAID of obtained delegated-prefix from the upstream interface.	integer	Minimum value: 0 Maximum value: 4294967295	0
ip6-subnet	Subnet to routing prefix. Syntax: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/xxx.	ipv6-prefix	Not Specified	::/0
dhcp6-relay-service	Enable/disable DHCPv6 relay.	option	-	disable
	<b>Option</b> <b>Description</b>			
	<i>disable</i>	Disable DHCPv6 relay		
	<i>enable</i>	Enable DHCPv6 relay.		
dhcp6-relay-type	DHCPv6 relay type.	option	-	regular

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>regular</i></td><td>Regular DHCP relay.</td></tr></table>	Option	Description	<i>regular</i>	Regular DHCP relay.							
Option	Description											
<i>regular</i>	Regular DHCP relay.											
dhcp6-relay-ip	DHCPv6 relay IP address.	user	Not Specified									
dhcp6-client-options	DHCPv6 client options.	option	-									
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>rapid</i></td><td>Send rapid commit option.</td></tr><tr><td><i>iapd</i></td><td>Send including IA-PD option.</td></tr><tr><td><i>iana</i></td><td>Send including IA-NA option.</td></tr></table>	Option	Description	<i>rapid</i>	Send rapid commit option.	<i>iapd</i>	Send including IA-PD option.	<i>iana</i>	Send including IA-NA option.			
Option	Description											
<i>rapid</i>	Send rapid commit option.											
<i>iapd</i>	Send including IA-PD option.											
<i>iana</i>	Send including IA-NA option.											
dhcp6-prefix-delegation	Enable/disable DHCPv6 prefix delegation.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable DHCPv6 prefix delegation.</td></tr><tr><td><i>disable</i></td><td>Disable DHCPv6 prefix delegation.</td></tr></table>	Option	Description	<i>enable</i>	Enable DHCPv6 prefix delegation.	<i>disable</i>	Disable DHCPv6 prefix delegation.					
Option	Description											
<i>enable</i>	Enable DHCPv6 prefix delegation.											
<i>disable</i>	Disable DHCPv6 prefix delegation.											
dhcp6-information-request	Enable/disable DHCPv6 information request.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable DHCPv6 information request.</td></tr><tr><td><i>disable</i></td><td>Disable DHCPv6 information request.</td></tr></table>	Option	Description	<i>enable</i>	Enable DHCPv6 information request.	<i>disable</i>	Disable DHCPv6 information request.					
Option	Description											
<i>enable</i>	Enable DHCPv6 information request.											
<i>disable</i>	Disable DHCPv6 information request.											
cli-conn6-status	CLI IPv6 connection status.	integer	Minimum value: 0 Maximum value: 4294967295	0								
vrrp-virtual-mac6	Enable/disable virtual MAC for VRRP.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable virtual MAC for VRRP.</td></tr><tr><td><i>disable</i></td><td>Disable virtual MAC for VRRP.</td></tr></table>	Option	Description	<i>enable</i>	Enable virtual MAC for VRRP.	<i>disable</i>	Disable virtual MAC for VRRP.					
Option	Description											
<i>enable</i>	Enable virtual MAC for VRRP.											
<i>disable</i>	Disable virtual MAC for VRRP.											
vrip6_link_local	Link-local IPv6 address of virtual router.	ipv6-address	Not Specified	::								

### config ip6-extra-addr

Parameter	Description	Type	Size	Default
prefix	IPv6 address prefix.	ipv6-prefix	Not Specified	::/0

### config ip6-prefix-list

Parameter	Description	Type	Size	Default
prefix	IPv6 prefix.	ipv6-network	Not Specified	::/0
autonomous-flag	Enable/disable the autonomous flag.	option	-	enable
	Option	Description		
	enable	Enable the autonomous flag.		
	disable	Disable the autonomous flag.		
onlink-flag	Enable/disable the onlink flag.	option	-	enable
	Option	Description		
	enable	Enable the onlink flag.		
	disable	Disable the onlink flag.		
valid-life-time	Valid life time (sec).	integer	Minimum value: 0 Maximum value: 4294967295	2592000
preferred-life-time	Preferred life time (sec).	integer	Minimum value: 0 Maximum value: 4294967295	604800
rdnss	Recursive DNS server option.	user	Not Specified	
dnssl <domain>	DNS search list option. Domain name.	string	Maximum length: 79	

## config ip6-delegated-prefix-list

Parameter	Description	Type	Size	Default								
prefix-id	Prefix ID.	integer	Minimum value: 0 Maximum value: 4294967295	0								
upstream-interface	Name of the interface that provides delegated information.	string	Maximum length: 15									
delegated-prefix-iaid	IAID of obtained delegated-prefix from the upstream interface.	integer	Minimum value: 0 Maximum value: 4294967295	0								
autonomous-flag	Enable/disable the autonomous flag.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable the autonomous flag.</td></tr><tr><td><i>disable</i></td><td>Disable the autonomous flag.</td></tr></table>	Option	Description	<i>enable</i>	Enable the autonomous flag.	<i>disable</i>	Disable the autonomous flag.					
Option	Description											
<i>enable</i>	Enable the autonomous flag.											
<i>disable</i>	Disable the autonomous flag.											
onlink-flag	Enable/disable the onlink flag.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable the onlink flag.</td></tr><tr><td><i>disable</i></td><td>Disable the onlink flag.</td></tr></table>	Option	Description	<i>enable</i>	Enable the onlink flag.	<i>disable</i>	Disable the onlink flag.					
Option	Description											
<i>enable</i>	Enable the onlink flag.											
<i>disable</i>	Disable the onlink flag.											
subnet	Add subnet ID to routing prefix.	ipv6-network	Not Specified	::/0								
rdnss-service	Recursive DNS service option.	option	-	specify								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>delegated</i></td><td>Delegated RDNSS settings.</td></tr><tr><td><i>default</i></td><td>System RDNSS settings.</td></tr><tr><td><i>specify</i></td><td>Specify recursive DNS servers.</td></tr></table>	Option	Description	<i>delegated</i>	Delegated RDNSS settings.	<i>default</i>	System RDNSS settings.	<i>specify</i>	Specify recursive DNS servers.			
Option	Description											
<i>delegated</i>	Delegated RDNSS settings.											
<i>default</i>	System RDNSS settings.											
<i>specify</i>	Specify recursive DNS servers.											
rdnss	Recursive DNS server option.	user	Not Specified									

### config dhcp6-iapd-list

Parameter	Description	Type	Size	Default
iaid	Identity association identifier.	integer	Minimum value: 0 Maximum value: 4294967295	0
prefix-hint	DHCPv6 prefix that will be used as a hint to the upstream DHCPv6 server.	ipv6-network	Not Specified	::/0
prefix-hint-plt	DHCPv6 prefix hint preferred life time (sec), 0 means unlimited lease time.	integer	Minimum value: 0 Maximum value: 4294967295	604800
prefix-hint-vlt	DHCPv6 prefix hint valid life time (sec).	integer	Minimum value: 0 Maximum value: 4294967295	2592000

### config vrrp6

Parameter	Description	Type	Size	Default
vrid	Virtual router identifier.	integer	Minimum value: 1 Maximum value: 255	0
vrgrp	VRRP group ID.	integer	Minimum value: 1 Maximum value: 65535	0
vip6	IPv6 address of the virtual router.	ipv6-address	Not Specified	::
priority	Priority of the virtual router.	integer	Minimum value: 1 Maximum value: 255	100
adv-interval	Advertisement interval.	integer	Minimum value: 1 Maximum value: 255	1

Parameter	Description	Type	Size	Default
start-time	Startup time.	integer	Minimum value: 1 Maximum value: 255	3
preempt	Enable/disable preempt mode.	option	-	enable
	Option	Description		
	enable	Enable preempt mode.		
	disable	Disable preempt mode.		
accept-mode	Enable/disable accept mode.	option	-	enable
	Option	Description		
	enable	Enable accept mode.		
	disable	Disable accept mode.		
vrdst6	Monitor the route to this destination.	ipv6-address	Not Specified	
status	Enable/disable VRRP.	option	-	enable
	Option	Description		
	enable	Enable VRRP.		
	disable	Disable VRRP.		

### config l2tp-client-settings

Parameter	Description	Type	Size	Default
user	L2TP user name.	string	Maximum length: 127	
password	L2TP password.	password	Not Specified	
peer-host	L2TP peer host address.	string	Maximum length: 255	
peer-mask	L2TP peer mask.	ipv4-netmask	Not Specified	255.255.255.255
peer-port	L2TP peer port number.	integer	Minimum value: 1 Maximum value: 65535	1701



Parameter	Description	Type	Size	Default
auth-type	L2TP authentication type.	option	-	auto
	<b>Option</b>	<b>Description</b>		
	<i>auto</i>	Automatically choose authentication.		
	<i>pap</i>	PAP authentication.		
	<i>chap</i>	CHAP authentication.		
	<i>mschapv1</i>	MS-CHAPv1 authentication.		
	<i>mschapv2</i>	MS-CHAPv2 authentication.		
mtu	L2TP MTU.	integer	Minimum value: 40 Maximum value: 65535	1460
distance	Distance of learned routes.	integer	Minimum value: 1 Maximum value: 255	2
priority	Priority of learned routes.	integer	Minimum value: 1 Maximum value: 65535	1
defaultgw	Enable/disable default gateway.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable default gateway.		
	<i>disable</i>	Disable default gateway.		
ip	IP.	ipv4-classnet-host	Not Specified	0.0.0.0 0.0.0.0
hello-interval	L2TP hello message interval in seconds.	integer	Minimum value: 0 Maximum value: 3600	60

## config secondaryip

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
ip	Secondary IP address of the interface.	ipv4-classnet-host	Not Specified	0.0.0.0 0.0.0.0
allowaccess	Management access settings for the secondary IP address.	option	-	
	<b>Option</b>	<b>Description</b>		
	ping	PING access.		
	https	HTTPS access.		
	ssh	SSH access.		
	snmp	SNMP access.		
	http	HTTP access.		
	telnet	TELNET access.		
	fgfm	FortiManager access.		
	radius-acct	RADIUS accounting access.		
	probe-response	Probe access.		
	fabric	Security Fabric access.		
	ftm	FTM access.		
	speed-test	Speed test access.		
gwdetect	Enable/disable detect gateway alive for first.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	enable	Enable detect gateway alive for first.		
	disable	Disable detect gateway alive for first.		
ping-serv-status	PING server status.	integer	Minimum value: 0 Maximum value: 255	0
detectserver	Gateway's ping server for this IP.	user	Not Specified	
detectprotocol	Protocols used to detect the server.	option	-	ping

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>ping</i>	PING.		
	<i>tcp-echo</i>	TCP echo.		
	<i>udp-echo</i>	UDP echo.		
ha-priority	HA election priority for the PING server.	integer	Minimum value: 1 Maximum value: 50	1

### config tagging

Parameter	Description	Type	Size	Default
name	Tagging entry name.	string	Maximum length: 63	
category	Tag category.	string	Maximum length: 63	
tags <name>	Tags. Tag name.	string	Maximum length: 79	

### config vrrp

Parameter	Description	Type	Size	Default
vrid	Virtual router identifier.	integer	Minimum value: 1 Maximum value: 255	0
version	VRRP version.	option	-	2
	Option	Description		
	2	VRRP version 2.		
	3	VRRP version 3.		
vrgrp	VRRP group ID.	integer	Minimum value: 1 Maximum value: 65535	0

Parameter	Description	Type	Size	Default						
vrip	IP address of the virtual router.	ipv4-address-any	Not Specified	0.0.0.0						
priority	Priority of the virtual router.	integer	Minimum value: 1 Maximum value: 255	100						
adv-interval	Advertisement interval.	integer	Minimum value: 1 Maximum value: 255	1						
start-time	Startup time.	integer	Minimum value: 1 Maximum value: 255	3						
preempt	Enable/disable preempt mode.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable preempt mode.</td></tr><tr><td>disable</td><td>Disable preempt mode.</td></tr></table>				Option	Description	enable	Enable preempt mode.	disable	Disable preempt mode.
Option	Description									
enable	Enable preempt mode.									
disable	Disable preempt mode.									
accept-mode	Enable/disable accept mode.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable accept mode.</td></tr><tr><td>disable</td><td>Disable accept mode.</td></tr></table>				Option	Description	enable	Enable accept mode.	disable	Disable accept mode.
Option	Description									
enable	Enable accept mode.									
disable	Disable accept mode.									
vrdst	Monitor the route to this destination.	ipv4-address-any	Not Specified							
vrdst-priority	Priority of the virtual router when the virtual router destination becomes unreachable.	integer	Minimum value: 0 Maximum value: 254	0						
ignore-default-route	Enable/disable ignoring of default route when checking destination.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable ignoring of default route when checking destination.</td></tr><tr><td>disable</td><td>Disable ignoring of default route when checking destination.</td></tr></table>				Option	Description	enable	Enable ignoring of default route when checking destination.	disable	Disable ignoring of default route when checking destination.
Option	Description									
enable	Enable ignoring of default route when checking destination.									
disable	Disable ignoring of default route when checking destination.									

Parameter	Description	Type	Size	Default
status	Enable/disable this VRRP configuration.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable this VRRP configuration.		
	<i>disable</i>	Disable this VRRP configuration.		

### config proxy-arp

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
ip	Set IP addresses of proxy ARP.	user	Not Specified	

### config wifi-mac-list

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
mac	MAC address.	mac-address	Not Specified	00:00:00:00:00:00

### config wifi-networks

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
wifi-ssid	IEEE 802.11 Service Set Identifier.	string	Maximum length: 32	fortinet
wifi-security	Wireless access security of SSID.	option	-	wpa-personal

Parameter	Description	Type	Size	Default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>open</i></td><td>Open.</td></tr><tr><td><i>wep64</i></td><td>WEP64.</td></tr><tr><td><i>wep128</i></td><td>WEP128.</td></tr><tr><td><i>wpa-personal</i></td><td>WPA personal.</td></tr><tr><td><i>wpa-only-personal</i></td><td>WPA personal only.</td></tr><tr><td><i>wpa2-only-personal</i></td><td>WPA2 personal only.</td></tr></table>	Option	Description	<i>open</i>	Open.	<i>wep64</i>	WEP64.	<i>wep128</i>	WEP128.	<i>wpa-personal</i>	WPA personal.	<i>wpa-only-personal</i>	WPA personal only.	<i>wpa2-only-personal</i>	WPA2 personal only.			
	Option	Description																
	<i>open</i>	Open.																
	<i>wep64</i>	WEP64.																
	<i>wep128</i>	WEP128.																
	<i>wpa-personal</i>	WPA personal.																
	<i>wpa-only-personal</i>	WPA personal only.																
<i>wpa2-only-personal</i>	WPA2 personal only.																	
wifi-encrypt	Data encryption.	option	-	AES														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>TKIP</i></td><td>TKIP.</td></tr><tr><td><i>AES</i></td><td>AES.</td></tr></table>	Option	Description	<i>TKIP</i>	TKIP.	<i>AES</i>	AES.											
	Option	Description																
	<i>TKIP</i>	TKIP.																
<i>AES</i>	AES.																	
wifi-keyindex	WEP key index.	integer	Minimum value: 1 Maximum value: 4	1														
wifi-key	WiFi WEP Key.	password	Not Specified															
wifi-passphrase	WiFi pre-shared key for WPA.	password	Not Specified															

## config system ipam

Configure IP address management services.

```
config system ipam
    Description: Configure IP address management services.
    set pool-subnet {ipv4-classnet}
    set server-type [cloud|fabric-root]
    set status [enable|disable]
end
```

## config system ipam

Parameter	Description	Type	Size	Default
pool-subnet	Configure IPAM pool subnet, Class A - Class B subnet.	ipv4-classnet	Not Specified	172.31.0.0 255.255.0.0

Parameter	Description	Type	Size	Default
server-type	Configure the type of IPAM server to use.	option	-	fabric-root
	<b>Option</b>	<b>Description</b>		
	<i>cloud</i>	Use the FortiIPAM cloud server.		
	<i>fabric-root</i>	Use the IPAM server running on the Security Fabric root.		
status	Enable/disable IP address management services.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable integration with IP address management services.		
	<i>disable</i>	Disable integration with IP address management services.		

## config system ipip-tunnel

Configure IP in IP Tunneling.

```
config system ipip-tunnel
    Description: Configure IP in IP Tunneling.
    edit <name>
        set auto-asic-offload [enable|disable]
        set interface {string}
        set local-gw {ipv4-address-any}
        set remote-gw {ipv4-address}
        set use-sdwan [disable|enable]
    next
end
```

## config system ipip-tunnel

Parameter	Description	Type	Size	Default
auto-asic-offload *	Enable/disable tunnel ASIC offloading.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable auto ASIC offloading.		
	<i>disable</i>	Disable ASIC offloading.		
interface	Interface name that is associated with the incoming traffic from available options.	string	Maximum length: 15	
local-gw	IPv4 address for the local gateway.	ipv4-address-any	Not Specified	0.0.0.0

Parameter	Description	Type	Size	Default
name	IPIP Tunnel name.	string	Maximum length: 15	
remote-gw	IPv4 address for the remote gateway.	ipv4-address	Not Specified	0.0.0.0
use-sdwan	Enable/disable use of SD-WAN to reach remote gateway.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable use of SD-WAN to reach remote gateway.		
	<i>enable</i>	Enable use of SD-WAN to reach remote gateway.		

\* This parameter may not exist in some models.

## config system ips-urlfilter-dns

Configure IPS URL filter DNS servers.

```
config system ips-urlfilter-dns
    Description: Configure IPS URL filter DNS servers.
    edit <address>
        set ipv6-capability [enable|disable]
        set status [enable|disable]
    next
end
```

## config system ips-urlfilter-dns

Parameter	Description	Type	Size	Default
address	DNS server IP address.	ipv4-address	Not Specified	0.0.0.0
ipv6-capability	Enable/disable this server for IPv6 queries.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
status	Enable/disable using this DNS server for IPS URL filter DNS queries.	option	-	enable



Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable this DNS server for IPS URL filter DNS queries.		
	<i>disable</i>	Disable this DNS server for IPS URL filter DNS queries.		

## config system ips-urlfilter-dns6

Configure IPS URL filter IPv6 DNS servers.

```
config system ips-urlfilter-dns6
    Description: Configure IPS URL filter IPv6 DNS servers.
    edit <address6>
        set status [enable|disable]
    next
end
```

## config system ips-urlfilter-dns6

Parameter	Description	Type	Size	Default
address6	IPv6 address of DNS server.	ipv6-address	Not Specified	::
status	Enable/disable this server for IPv6 DNS queries.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

## config system ips

Configure IPS system settings.

```
config system ips
    Description: Configure IPS system settings.
    set override-signature-hold-by-id [enable|disable]
    set signature-hold-time {user}
end
```

## config system ips

Parameter	Description	Type	Size	Default
override-signature-hold-by-id	Enable/disable override of hold of triggering signatures that are specified by IDs regardless of hold.	option	-	enable
	Option	Description		
	<i>enable</i>	Allow the signatures specified by IDs to be triggered even if they are on hold.		
	<i>disable</i>	Do not trigger the signatures that are on hold.		
signature-hold-time	Time to hold and monitor IPS signatures. Format <#d##h>.	user	Not Specified	0h

## config system ipsec-aggregate

Configure an aggregate of IPsec tunnels.

```
config system ipsec-aggregate
    Description: Configure an aggregate of IPsec tunnels.
    edit <name>
        set algorithm [L3|L4|...]
        set member <tunnel-name1>, <tunnel-name2>, ...
    next
end
```

## config system ipsec-aggregate

Parameter	Description	Type	Size	Default
algorithm	Frame distribution algorithm.	option	-	round-robin
	<b>Option</b>	<b>Description</b>		
	<i>L3</i>	Use layer 3 address for distribution.		
	<i>L4</i>	Use layer 4 information for distribution.		
	<i>round-robin</i>	Per-packet round-robin distribution.		
	<i>redundant</i>	Use first tunnel that is up for all traffic.		
	<i>weighted-round-robin</i>	Weighted round-robin distribution.		
member <tunnel-name>	Member tunnels of the aggregate. Tunnel name.	string	Maximum length: 79	

Parameter	Description	Type	Size	Default
name	IPsec aggregate name.	string	Maximum length: 15	

## config system ipv6-neighbor-cache

Configure IPv6 neighbor cache table.

```
config system ipv6-neighbor-cache
    Description: Configure IPv6 neighbor cache table.
    edit <id>
        set interface {string}
        set ipv6 {ipv6-address}
        set mac {mac-address}
    next
end
```

## config system ipv6-neighbor-cache

Parameter	Description	Type	Size	Default
id	Unique integer ID of the entry.	integer	Minimum value: 0 Maximum value: 4294967295	0
interface	Select the associated interface name from available options.	string	Maximum length: 15	
ipv6	IPv6 address (format: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx).	ipv6-address	Not Specified	::
mac	MAC address (format: xx:xx:xx:xx:xx:xx).	mac-address	Not Specified	00:00:00:00:00:00

## config system ipv6-tunnel

Configure IPv6/IPv4 in IPv6 tunnel.

```
config system ipv6-tunnel
    Description: Configure IPv6/IPv4 in IPv6 tunnel.
    edit <name>
        set auto-asic-offload [enable|disable]
        set destination {ipv6-address}
        set interface {string}
        set source {ipv6-address}
        set use-sdwan [disable|enable]
    next
end
```

## config system ipv6-tunnel

Parameter	Description	Type	Size	Default
auto-asic-offload *	Enable/disable tunnel ASIC offloading.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable auto ASIC offloading.		
	<i>disable</i>	Disable ASIC offloading.		
destination	Remote IPv6 address of the tunnel.	ipv6-address	Not Specified	::
interface	Interface name.	string	Maximum length: 15	
name	IPv6 tunnel name.	string	Maximum length: 15	
source	Local IPv6 address of the tunnel.	ipv6-address	Not Specified	::
use-sdwan	Enable/disable use of SD-WAN to reach remote gateway.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable use of SD-WAN to reach remote gateway.		
	<i>enable</i>	Enable use of SD-WAN to reach remote gateway.		

\* This parameter may not exist in some models.

## config system isf-queue-profile



This command is available for model(s): FortiGate 1200D, FortiGate 1500DT, FortiGate 1500D, FortiGate 3000D, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3700D, FortiGate 400E, FortiGate 401E, FortiGate 800D.

It is not available for: FortiGate 1000D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 140E-POE, FortiGate 140E, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000F, FortiGate 3001F, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3800D, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400F, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

Create a queue profile of switch.

```
config system isf-queue-profile
  Description: Create a queue profile of switch.
  edit <name>
    set bandwidth-unit [kbps|pps]
    set burst-bps-granularity [disable|512-bytes|...]
    set burst-pps-granularity [disable|half-packet|...]
    set guaranteed-bandwidth {integer}
    set maximum-bandwidth {integer}
  next
end
```

## config system isf-queue-profile

Parameter	Description	Type	Size	Default
bandwidth-unit	Unit of measurement for guaranteed and maximum bandwidth.	option	-	kbps
	Option	Description		
	<i>kbps</i>	kilobits per second.		
	<i>pps</i>	packets per second.		

Parameter	Description	Type	Size	Default																		
burst-bps-granularity	Burst granularity based on bytes per second.	option	-	disable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable burst control.</td></tr><tr><td><i>512-bytes</i></td><td>512 bytes.</td></tr><tr><td><i>1k-bytes</i></td><td>1K bytes.</td></tr><tr><td><i>2k-bytes</i></td><td>2K bytes.</td></tr><tr><td><i>4k-bytes</i></td><td>4K bytes.</td></tr><tr><td><i>8k-bytes</i></td><td>8K bytes.</td></tr><tr><td><i>16k-bytes</i></td><td>16K bytes.</td></tr><tr><td><i>32k-bytes</i></td><td>32K bytes.</td></tr></table>	Option	Description	<i>disable</i>	Disable burst control.	<i>512-bytes</i>	512 bytes.	<i>1k-bytes</i>	1K bytes.	<i>2k-bytes</i>	2K bytes.	<i>4k-bytes</i>	4K bytes.	<i>8k-bytes</i>	8K bytes.	<i>16k-bytes</i>	16K bytes.	<i>32k-bytes</i>	32K bytes.			
	Option	Description																				
	<i>disable</i>	Disable burst control.																				
	<i>512-bytes</i>	512 bytes.																				
	<i>1k-bytes</i>	1K bytes.																				
	<i>2k-bytes</i>	2K bytes.																				
	<i>4k-bytes</i>	4K bytes.																				
	<i>8k-bytes</i>	8K bytes.																				
	<i>16k-bytes</i>	16K bytes.																				
<i>32k-bytes</i>	32K bytes.																					
burst-pps-granularity	Burst granularity based on packets per second.	option	-	disable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable burst control.</td></tr><tr><td><i>half-packet</i></td><td>One burst unit equals two time slots in which one packet is sent.</td></tr><tr><td><i>1-packet</i></td><td>1 packet.</td></tr><tr><td><i>2-packets</i></td><td>2 packets.</td></tr><tr><td><i>4-packets</i></td><td>4 packets.</td></tr><tr><td><i>16-packets</i></td><td>16 packets.</td></tr><tr><td><i>65-packets</i></td><td>65 packets.</td></tr><tr><td><i>262-packets</i></td><td>262 packets.</td></tr></table>	Option	Description	<i>disable</i>	Disable burst control.	<i>half-packet</i>	One burst unit equals two time slots in which one packet is sent.	<i>1-packet</i>	1 packet.	<i>2-packets</i>	2 packets.	<i>4-packets</i>	4 packets.	<i>16-packets</i>	16 packets.	<i>65-packets</i>	65 packets.	<i>262-packets</i>	262 packets.			
	Option	Description																				
	<i>disable</i>	Disable burst control.																				
	<i>half-packet</i>	One burst unit equals two time slots in which one packet is sent.																				
	<i>1-packet</i>	1 packet.																				
	<i>2-packets</i>	2 packets.																				
	<i>4-packets</i>	4 packets.																				
	<i>16-packets</i>	16 packets.																				
	<i>65-packets</i>	65 packets.																				
<i>262-packets</i>	262 packets.																					
guaranteed-bandwidth	Guaranteed bandwidth.	integer	Minimum value: 0 Maximum value: 100000000	0																		
maximum-bandwidth	Upper bandwidth limit enforced.	integer	Minimum value: 0 Maximum value: 100000000	0																		
name	Profile name.	string	Maximum length: 15																			

---

## config system link-monitor

Configure Link Health Monitor.

```
config system link-monitor
  Description: Configure Link Health Monitor.
  edit <name>
    set addr-mode [ipv4|ipv6]
    set class-id {integer}
    set diffservcode {user}
    set fail-weight {integer}
    set failtime {integer}
    set gateway-ip {ipv4-address-any}
    set gateway-ip6 {ipv6-address}
    set ha-priority {integer}
    set http-agent {string}
    set http-get {string}
    set http-match {string}
    set interval {integer}
    set packet-size {integer}
    set password {password}
    set port {integer}
    set probe-count {integer}
    set probe-timeout {integer}
    set protocol {option1}, {option2}, ...
    set recoverytime {integer}
    set route <subnet1>, <subnet2>, ...
    set security-mode [none|authentication]
    set server <address1>, <address2>, ...
    set server-config [default|individual]
  config server-list
    Description: Servers for link-monitor to monitor.
    edit <id>
      set dst {string}
      set protocol {option1}, {option2}, ...
      set port {integer}
      set weight {integer}
    next
  end
  set service-detection [enable|disable]
  set source-ip {ipv4-address-any}
  set source-ip6 {ipv6-address}
  set srcintf {string}
  set status [enable|disable]
  set update-cascade-interface [enable|disable]
  set update-policy-route [enable|disable]
  set update-static-route [enable|disable]
next
end
```

## config system link-monitor

Parameter	Description	Type	Size	Default
addr-mode	Address mode (IPv4 or IPv6).	option	-	ipv4
	Option	Description		
	ipv4	IPv4 mode.		
	ipv6	IPv6 mode.		
class-id	Traffic class ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
diffservcode	Differentiated services code point (DSCP) in the IP header of the probe packet.	user	Not Specified	
fail-weight	Threshold weight to trigger link failure alert.	integer	Minimum value: 0 Maximum value: 255	0
failtime	Number of retry attempts before the server is considered down.	integer	Minimum value: 1 Maximum value: 3600	5
gateway-ip	Gateway IP address used to probe the server.	ipv4-address-any	Not Specified	0.0.0.0
gateway-ip6	Gateway IPv6 address used to probe the server.	ipv6-address	Not Specified	::
ha-priority	HA election priority.	integer	Minimum value: 1 Maximum value: 50	1
http-agent	String in the http-agent field in the HTTP header.	string	Maximum length: 1024	Chrome/ Safari/
http-get	If you are monitoring an HTML server you can send an HTTP-GET request with a custom string. Use this option to define the string.	string	Maximum length: 1024	/
http-match	String that you expect to see in the HTTP-GET requests of the traffic to be monitored.	string	Maximum length: 1024	



Parameter	Description	Type	Size	Default												
interval	Detection interval in milliseconds.	integer	Minimum value: 20 Maximum value: 3600000	500												
name	Link monitor name.	string	Maximum length: 35													
packet-size	Packet size of a TWAMP test session.	integer	Minimum value: 64 Maximum value: 1024	64												
password	TWAMP controller password in authentication mode.	password	Not Specified													
port	Port number of the traffic to be used to monitor the server.	integer	Minimum value: 1 Maximum value: 65535	0												
probe-count	Number of most recent probes that should be used to calculate latency and jitter.	integer	Minimum value: 5 Maximum value: 30	30												
probe-timeout	Time to wait before a probe packet is considered lost.	integer	Minimum value: 20 Maximum value: 5000	500												
protocol	Protocols used to monitor the server.	option	-	ping												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ping</i></td><td>PING link monitor.</td></tr><tr><td><i>tcp-echo</i></td><td>TCP echo link monitor.</td></tr><tr><td><i>udp-echo</i></td><td>UDP echo link monitor.</td></tr><tr><td><i>http</i></td><td>HTTP-GET link monitor.</td></tr><tr><td><i>twamp</i></td><td>TWAMP link monitor.</td></tr></table>				Option	Description	<i>ping</i>	PING link monitor.	<i>tcp-echo</i>	TCP echo link monitor.	<i>udp-echo</i>	UDP echo link monitor.	<i>http</i>	HTTP-GET link monitor.	<i>twamp</i>	TWAMP link monitor.
Option	Description															
<i>ping</i>	PING link monitor.															
<i>tcp-echo</i>	TCP echo link monitor.															
<i>udp-echo</i>	UDP echo link monitor.															
<i>http</i>	HTTP-GET link monitor.															
<i>twamp</i>	TWAMP link monitor.															
recoverytime	Number of successful responses received before server is considered recovered.	integer	Minimum value: 1 Maximum value: 3600	5												
route <subnet>	Subnet to monitor. IP and netmask (x.x.x.x/y).	string	Maximum length: 79													

Parameter	Description	Type	Size	Default						
security-mode	Twamp controller security mode.	option	-	none						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>Unauthenticated mode.</td></tr><tr><td><i>authentication</i></td><td>Authenticated mode.</td></tr></table>				Option	Description	<i>none</i>	Unauthenticated mode.	<i>authentication</i>	Authenticated mode.
	Option	Description								
	<i>none</i>	Unauthenticated mode.								
<i>authentication</i>	Authenticated mode.									
server <address>	IP address of the server(s) to be monitored. Server address.	string	Maximum length: 79							
server-config	Mode of server configuration.	option	-	default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>All servers share the same attributes.</td></tr><tr><td><i>individual</i></td><td>Some attributes can be specified for individual servers.</td></tr></table>				Option	Description	<i>default</i>	All servers share the same attributes.	<i>individual</i>	Some attributes can be specified for individual servers.
	Option	Description								
	<i>default</i>	All servers share the same attributes.								
<i>individual</i>	Some attributes can be specified for individual servers.									
service- detection	Only use monitor to read quality values. If enabled, static routes and cascade interfaces will not be updated.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Only use monitor for service-detection.</td></tr><tr><td><i>disable</i></td><td>Monitor will update routes/interfaces on link failure.</td></tr></table>				Option	Description	<i>enable</i>	Only use monitor for service-detection.	<i>disable</i>	Monitor will update routes/interfaces on link failure.
	Option	Description								
	<i>enable</i>	Only use monitor for service-detection.								
<i>disable</i>	Monitor will update routes/interfaces on link failure.									
source-ip	Source IP address used in packet to the server.	ipv4- address- any	Not Specified	0.0.0.0						
source-ip6	Source IPv6 address used in packet to the server.	ipv6- address	Not Specified	::						
srcintf	Interface that receives the traffic to be monitored.	string	Maximum length: 15							
status	Enable/disable this link monitor.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable this link monitor.</td></tr><tr><td><i>disable</i></td><td>Disable this link monitor.</td></tr></table>				Option	Description	<i>enable</i>	Enable this link monitor.	<i>disable</i>	Disable this link monitor.
	Option	Description								
	<i>enable</i>	Enable this link monitor.								
<i>disable</i>	Disable this link monitor.									
update- cascade- interface	Enable/disable update cascade interface.	option	-	enable						

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable update cascade interface.		
	<i>disable</i>	Disable update cascade interface.		
update-policy-route	Enable/disable updating the policy route.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable updating the policy route.		
	<i>disable</i>	Disable updating the policy route.		
update-static-route	Enable/disable updating the static route.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable updating the static route.		
	<i>disable</i>	Disable updating the static route.		

### config server-list

Parameter	Description	Type	Size	Default
id	Server ID.	integer	Minimum value: 1 Maximum value: 32	0
dst	IP address of the server to be monitored.	string	Maximum length: 64	
protocol	Protocols used to monitor the server.	option	-	ping
	<b>Option</b>	<b>Description</b>		
	<i>ping</i>	PING link monitor.		
	<i>tcp-echo</i>	TCP echo link monitor.		
	<i>udp-echo</i>	UDP echo link monitor.		
	<i>http</i>	HTTP-GET link monitor.		
	<i>twamp</i>	TWAMP link monitor.		

Parameter	Description	Type	Size	Default
port	Port number of the traffic to be used to monitor the server.	integer	Minimum value: 1 Maximum value: 65535	0
weight	Weight of the monitor to this dst.	integer	Minimum value: 0 Maximum value: 255	0

## config system lldp network-policy

Configure LLDP network policy.

```

config system lldp network-policy
    Description: Configure LLDP network policy.
    edit <name>
        set comment {var-string}
        config guest
            Description: Guest.
            set status [disable|enable]
            set tag [none|dot1q|...]
            set vlan {integer}
            set priority {integer}
            set dscp {integer}
        end
        config guest-voice-signaling
            Description: Guest Voice Signaling.
            set status [disable|enable]
            set tag [none|dot1q|...]
            set vlan {integer}
            set priority {integer}
            set dscp {integer}
        end
        config softphone
            Description: Softphone.
            set status [disable|enable]
            set tag [none|dot1q|...]
            set vlan {integer}
            set priority {integer}
            set dscp {integer}
        end
        config streaming-video
            Description: Streaming Video.
            set status [disable|enable]
            set tag [none|dot1q|...]
            set vlan {integer}
            set priority {integer}
            set dscp {integer}
        end
        config video-conferencing

```

```

        Description: Video Conferencing.
        set status [disable|enable]
        set tag [none|dot1q|...]
        set vlan {integer}
        set priority {integer}
        set dscp {integer}
    end
    config video-signaling
        Description: Video Signaling.
        set status [disable|enable]
        set tag [none|dot1q|...]
        set vlan {integer}
        set priority {integer}
        set dscp {integer}
    end
    config voice
        Description: Voice.
        set status [disable|enable]
        set tag [none|dot1q|...]
        set vlan {integer}
        set priority {integer}
        set dscp {integer}
    end
    config voice-signaling
        Description: Voice signaling.
        set status [disable|enable]
        set tag [none|dot1q|...]
        set vlan {integer}
        set priority {integer}
        set dscp {integer}
    end
end
next
end

```

## config system lldp network-policy

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 1023	
name	LLDP network policy name.	string	Maximum length: 35	

## config guest

Parameter	Description	Type	Size	Default
status	Enable/disable advertising this policy.	option	-	disable

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable advertising this LLDP network policy.		
	<i>enable</i>	Enable advertising this LLDP network policy.		
tag	Advertise tagged or untagged traffic.	option	-	none
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	Advertise that untagged frames should be used.		
	<i>dot1q</i>	Advertise that 802.1Q (VLAN) tagging should be used.		
	<i>dot1p</i>	Advertise that 802.1P priority tagging (VLAN 0) should be used.		
vlan	802.1Q VLAN ID to advertise.	integer	Minimum value: 1 Maximum value: 4094	0
priority	802.1P CoS/PCP to advertise.	integer	Minimum value: 0 Maximum value: 7	5
dscp	Differentiated Services Code Point (DSCP) value to advertise.	integer	Minimum value: 0 Maximum value: 63	46

### config guest-voice-signaling

Parameter	Description	Type	Size	Default
status	Enable/disable advertising this policy.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable advertising this LLDP network policy.		
	<i>enable</i>	Enable advertising this LLDP network policy.		
tag	Advertise tagged or untagged traffic.	option	-	none
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	Advertise that untagged frames should be used.		
	<i>dot1q</i>	Advertise that 802.1Q (VLAN) tagging should be used.		
	<i>dot1p</i>	Advertise that 802.1P priority tagging (VLAN 0) should be used.		

Parameter	Description	Type	Size	Default
vlan	802.1Q VLAN ID to advertise.	integer	Minimum value: 1 Maximum value: 4094	0
priority	802.1P CoS/PCP to advertise.	integer	Minimum value: 0 Maximum value: 7	5
dscp	Differentiated Services Code Point (DSCP) value to advertise.	integer	Minimum value: 0 Maximum value: 63	46

### config softphone

Parameter	Description	Type	Size	Default								
status	Enable/disable advertising this policy.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable advertising this LLDP network policy.</td></tr><tr><td>enable</td><td>Enable advertising this LLDP network policy.</td></tr></table>	Option	Description	disable	Disable advertising this LLDP network policy.	enable	Enable advertising this LLDP network policy.					
Option	Description											
disable	Disable advertising this LLDP network policy.											
enable	Enable advertising this LLDP network policy.											
tag	Advertise tagged or untagged traffic.	option	-	none								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>none</td><td>Advertise that untagged frames should be used.</td></tr><tr><td>dot1q</td><td>Advertise that 802.1Q (VLAN) tagging should be used.</td></tr><tr><td>dot1p</td><td>Advertise that 802.1P priority tagging (VLAN 0) should be used.</td></tr></table>	Option	Description	none	Advertise that untagged frames should be used.	dot1q	Advertise that 802.1Q (VLAN) tagging should be used.	dot1p	Advertise that 802.1P priority tagging (VLAN 0) should be used.			
Option	Description											
none	Advertise that untagged frames should be used.											
dot1q	Advertise that 802.1Q (VLAN) tagging should be used.											
dot1p	Advertise that 802.1P priority tagging (VLAN 0) should be used.											
vlan	802.1Q VLAN ID to advertise.	integer	Minimum value: 1 Maximum value: 4094	0								
priority	802.1P CoS/PCP to advertise.	integer	Minimum value: 0 Maximum value: 7	5								
dscp	Differentiated Services Code Point (DSCP) value to advertise.	integer	Minimum value: 0 Maximum value: 63	46								

## config streaming-video

Parameter	Description	Type	Size	Default
status	Enable/disable advertising this policy.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable advertising this LLDP network policy.		
	<i>enable</i>	Enable advertising this LLDP network policy.		
tag	Advertise tagged or untagged traffic.	option	-	none
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	Advertise that untagged frames should be used.		
	<i>dot1q</i>	Advertise that 802.1Q (VLAN) tagging should be used.		
	<i>dot1p</i>	Advertise that 802.1P priority tagging (VLAN 0) should be used.		
vlan	802.1Q VLAN ID to advertise.	integer	Minimum value: 1 Maximum value: 4094	0
priority	802.1P CoS/PCP to advertise.	integer	Minimum value: 0 Maximum value: 7	5
dscp	Differentiated Services Code Point (DSCP) value to advertise.	integer	Minimum value: 0 Maximum value: 63	46

## config video-conferencing

Parameter	Description	Type	Size	Default
status	Enable/disable advertising this policy.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable advertising this LLDP network policy.		
	<i>enable</i>	Enable advertising this LLDP network policy.		
tag	Advertise tagged or untagged traffic.	option	-	none



Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	Advertise that untagged frames should be used.		
	<i>dot1q</i>	Advertise that 802.1Q (VLAN) tagging should be used.		
	<i>dot1p</i>	Advertise that 802.1P priority tagging (VLAN 0) should be used.		
vlan	802.1Q VLAN ID to advertise.	integer	Minimum value: 1 Maximum value: 4094	0
priority	802.1P CoS/PCP to advertise.	integer	Minimum value: 0 Maximum value: 7	5
dscp	Differentiated Services Code Point (DSCP) value to advertise.	integer	Minimum value: 0 Maximum value: 63	46

### config video-signaling

Parameter	Description	Type	Size	Default
status	Enable/disable advertising this policy.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable advertising this LLDP network policy.		
	<i>enable</i>	Enable advertising this LLDP network policy.		
tag	Advertise tagged or untagged traffic.	option	-	none
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	Advertise that untagged frames should be used.		
	<i>dot1q</i>	Advertise that 802.1Q (VLAN) tagging should be used.		
	<i>dot1p</i>	Advertise that 802.1P priority tagging (VLAN 0) should be used.		
vlan	802.1Q VLAN ID to advertise.	integer	Minimum value: 1 Maximum value: 4094	0

Parameter	Description	Type	Size	Default
priority	802.1P CoS/PCP to advertise.	integer	Minimum value: 0 Maximum value: 7	5
dscp	Differentiated Services Code Point (DSCP) value to advertise.	integer	Minimum value: 0 Maximum value: 63	46

## config voice

Parameter	Description	Type	Size	Default
status	Enable/disable advertising this policy.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable advertising this LLDP network policy.		
	<i>enable</i>	Enable advertising this LLDP network policy.		
tag	Advertise tagged or untagged traffic.	option	-	none
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	Advertise that untagged frames should be used.		
	<i>dot1q</i>	Advertise that 802.1Q (VLAN) tagging should be used.		
	<i>dot1p</i>	Advertise that 802.1P priority tagging (VLAN 0) should be used.		
vlan	802.1Q VLAN ID to advertise.	integer	Minimum value: 1 Maximum value: 4094	0
priority	802.1P CoS/PCP to advertise.	integer	Minimum value: 0 Maximum value: 7	5
dscp	Differentiated Services Code Point (DSCP) value to advertise.	integer	Minimum value: 0 Maximum value: 63	46

## config voice-signaling

Parameter	Description	Type	Size	Default
status	Enable/disable advertising this policy.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable advertising this LLDP network policy.		
	<i>enable</i>	Enable advertising this LLDP network policy.		
tag	Advertise tagged or untagged traffic.	option	-	none
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	Advertise that untagged frames should be used.		
	<i>dot1q</i>	Advertise that 802.1Q (VLAN) tagging should be used.		
	<i>dot1p</i>	Advertise that 802.1P priority tagging (VLAN 0) should be used.		
vlan	802.1Q VLAN ID to advertise.	integer	Minimum value: 1 Maximum value: 4094	0
priority	802.1P CoS/PCP to advertise.	integer	Minimum value: 0 Maximum value: 7	5
dscp	Differentiated Services Code Point (DSCP) value to advertise.	integer	Minimum value: 0 Maximum value: 63	46

---

## config system lte-modem

---



This command is available for model(s): FortiGate 1000D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3900E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate VM64.

---

### Configure USB LTE/WIMAX devices.

```
config system lte-modem
    Description: Configure USB LTE/WIMAX devices.
    set allow-modify-mtu-size [enable|disable]
    set allow-modify-wireless-profile-table [enable|disable]
    set apn {string}
    set authtype [none|pap|...]
    set auto-connect [enable|disable]
    set band-restrictions {string}
    set billing-date {integer}
    set connection-hot-swap [5-minutes|10-minutes|...]
    set data-limit {integer}
    set data-usage-tracking [enable|disable]
    set extra-init {string}
    set force-wireless-profile {integer}
    set gps-port {integer}
    set gps-service [enable|disable]
    set holddown-timer {integer}
    set image-preference [generic|att|...]
    set interface {string}
    set manual-handover [enable|disable]
    set mode [standalone|redundant]
    set modem-port {integer}
    set network-type [auto|umts-3g|...]
    set override-gateway [enable|disable]
    set passwd {password}
```

```

set sim-hot-swap [enable|disable]
set sim-slot {integer}
set sim1-pin {password}
set sim2-pin {password}
set status [enable|disable]
set username {string}
end

```

## config system lte-modem

Parameter	Description	Type	Size	Default								
allow-modify-mtu-size *	Allow FortiGate to modify the wireless WAN interface MTU size.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Allow LTE daemon to modify wireless profile table.</td></tr><tr><td><i>disable</i></td><td>Do not allow LTE daemon to modify wireless profile table.</td></tr></table>	Option	Description	<i>enable</i>	Allow LTE daemon to modify wireless profile table.	<i>disable</i>	Do not allow LTE daemon to modify wireless profile table.					
Option	Description											
<i>enable</i>	Allow LTE daemon to modify wireless profile table.											
<i>disable</i>	Do not allow LTE daemon to modify wireless profile table.											
allow-modify-wireless-profile-table *	Allow FortiGate to modify the wireless profile table if the internal LTE modem is running the GENERIC modem firmware.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Allow LTE daemon to modify wireless profile table.</td></tr><tr><td><i>disable</i></td><td>Do not allow LTE daemon to modify wireless profile table.</td></tr></table>	Option	Description	<i>enable</i>	Allow LTE daemon to modify wireless profile table.	<i>disable</i>	Do not allow LTE daemon to modify wireless profile table.					
Option	Description											
<i>enable</i>	Allow LTE daemon to modify wireless profile table.											
<i>disable</i>	Do not allow LTE daemon to modify wireless profile table.											
apn	Login APN string for PDP-IP packet data calls.	string	Maximum length: 127									
authtype	Authentication type for PDP-IP packet data calls.	option	-	none								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>Username and password not required.</td></tr><tr><td><i>pap</i></td><td>Use PAP authentication.</td></tr><tr><td><i>chap</i></td><td>Use CHAP authentication.</td></tr></table>	Option	Description	<i>none</i>	Username and password not required.	<i>pap</i>	Use PAP authentication.	<i>chap</i>	Use CHAP authentication.			
Option	Description											
<i>none</i>	Username and password not required.											
<i>pap</i>	Use PAP authentication.											
<i>chap</i>	Use CHAP authentication.											
auto-connect *	Enable/disable modem auto connect.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable modem auto connect.</td></tr><tr><td><i>disable</i></td><td>Disable modem auto connect.</td></tr></table>	Option	Description	<i>enable</i>	Enable modem auto connect.	<i>disable</i>	Disable modem auto connect.					
Option	Description											
<i>enable</i>	Enable modem auto connect.											
<i>disable</i>	Disable modem auto connect.											

Parameter	Description	Type	Size	Default								
band-restrictions *	Bitmaps for the allowed 3G and LTE bands.Ex: 0000000000000000-0000000000001008 (3G Mask-LTE Mask)	string	Maximum length: 35									
billing-date *	LTE Modem billing date.	integer	Minimum value: 1 Maximum value: 31	1								
connection-hot-swap *	Set connection-based SIM card hot swap time interval.	option	-	5-minutes								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>5-minutes</td><td>Perform SIM card hot swap if current card is not able to connect for 5 minutes.</td></tr><tr><td>10-minutes</td><td>Perform SIM card hot swap if current card is not able to connect for 10 minutes.</td></tr><tr><td>never</td><td>SIM card hot swap based on card presence only.</td></tr></table>				Option	Description	5-minutes	Perform SIM card hot swap if current card is not able to connect for 5 minutes.	10-minutes	Perform SIM card hot swap if current card is not able to connect for 10 minutes.	never	SIM card hot swap based on card presence only.
Option	Description											
5-minutes	Perform SIM card hot swap if current card is not able to connect for 5 minutes.											
10-minutes	Perform SIM card hot swap if current card is not able to connect for 10 minutes.											
never	SIM card hot swap based on card presence only.											
data-limit *	LTE Modem data limit mega bytes, 0 for unlimited data.	integer	Minimum value: 0 Maximum value: 100000	0								
data-usage-tracking *	Enable/disable data usage tracking.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable data usage tracking.</td></tr><tr><td>disable</td><td>Disable data usage tracking.</td></tr></table>				Option	Description	enable	Enable data usage tracking.	disable	Disable data usage tracking.		
Option	Description											
enable	Enable data usage tracking.											
disable	Disable data usage tracking.											
extra-init	Extra initialization string for USB LTE/WIMAX devices.	string	Maximum length: 127									
force-wireless-profile *	Force to use wireless profile index , 0 if don't force.	integer	Minimum value: 0 Maximum value: 16	0								
gps-port *	Modem GPS port index.	integer	Minimum value: 0 Maximum value: 20	255								
gps-service *	Enable/disable GPS daemon.	option	-	enable								

Parameter	Description	Type	Size	Default																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable GPS daemon.</td></tr><tr><td><i>disable</i></td><td>Disable GPS daemon.</td></tr></table>				Option	Description	<i>enable</i>	Enable GPS daemon.	<i>disable</i>	Disable GPS daemon.														
	Option	Description																						
	<i>enable</i>	Enable GPS daemon.																						
<i>disable</i>	Disable GPS daemon.																							
holddown-timer	Hold down timer.	integer	Minimum value: 10 Maximum value: 60	30																				
image-preference *	Modem Image Preference.	option	-	auto-sim																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>generic</i></td><td>Generic Firmware.</td></tr><tr><td><i>att</i></td><td>AT&amp;T Firmware.</td></tr><tr><td><i>verizon</i></td><td>Verizon Firmware.</td></tr><tr><td><i>telus</i></td><td>Telus Firmware.</td></tr><tr><td><i>docomo</i></td><td>DOCOMO Firmware.</td></tr><tr><td><i>softbank</i></td><td>Softbank Firmware.</td></tr><tr><td><i>sprint</i></td><td>Sprint Firmware.</td></tr><tr><td><i>auto-sim</i></td><td>Auto Select Firmware.</td></tr><tr><td><i>no-change</i></td><td>Do not change.</td></tr></table>				Option	Description	<i>generic</i>	Generic Firmware.	<i>att</i>	AT&T Firmware.	<i>verizon</i>	Verizon Firmware.	<i>telus</i>	Telus Firmware.	<i>docomo</i>	DOCOMO Firmware.	<i>softbank</i>	Softbank Firmware.	<i>sprint</i>	Sprint Firmware.	<i>auto-sim</i>	Auto Select Firmware.	<i>no-change</i>	Do not change.
	Option	Description																						
	<i>generic</i>	Generic Firmware.																						
	<i>att</i>	AT&T Firmware.																						
	<i>verizon</i>	Verizon Firmware.																						
	<i>telus</i>	Telus Firmware.																						
	<i>docomo</i>	DOCOMO Firmware.																						
	<i>softbank</i>	Softbank Firmware.																						
	<i>sprint</i>	Sprint Firmware.																						
<i>auto-sim</i>	Auto Select Firmware.																							
<i>no-change</i>	Do not change.																							
interface	The interface that the modem is acting as a redundant interface for.	string	Maximum length: 63																					
manual-handover *	Enable/Disable manual handover from 3G to LTE network.	option	-	disable																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable 3G to LTE manual handover.</td></tr><tr><td><i>disable</i></td><td>Disable 3G to LTE manual handover.</td></tr></table>				Option	Description	<i>enable</i>	Enable 3G to LTE manual handover.	<i>disable</i>	Disable 3G to LTE manual handover.														
	Option	Description																						
	<i>enable</i>	Enable 3G to LTE manual handover.																						
<i>disable</i>	Disable 3G to LTE manual handover.																							
mode	Modem operation mode.	option	-	standalone																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>standalone</i></td><td>Standalone modem operation mode.</td></tr><tr><td><i>redundant</i></td><td>Redundant modem operation mode where the modem is used as a backup interface.</td></tr></table>				Option	Description	<i>standalone</i>	Standalone modem operation mode.	<i>redundant</i>	Redundant modem operation mode where the modem is used as a backup interface.														
	Option	Description																						
	<i>standalone</i>	Standalone modem operation mode.																						
<i>redundant</i>	Redundant modem operation mode where the modem is used as a backup interface.																							

Parameter	Description	Type	Size	Default										
modem-port	Modem port index.	integer	Minimum value: 0 Maximum value: 20	255										
network-type *	Wireless network type.	option	-	auto										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>auto</td><td>Automatic detection</td></tr><tr><td>umts-3g</td><td>UMTS 3G -- For networks use GSM technology</td></tr><tr><td>lte</td><td>LTE</td></tr><tr><td>cdma-hrpd</td><td>CDMA and HRPD -- For networks use CDMA technology</td></tr></table>	Option	Description	auto	Automatic detection	umts-3g	UMTS 3G -- For networks use GSM technology	lte	LTE	cdma-hrpd	CDMA and HRPD -- For networks use CDMA technology			
Option	Description													
auto	Automatic detection													
umts-3g	UMTS 3G -- For networks use GSM technology													
lte	LTE													
cdma-hrpd	CDMA and HRPD -- For networks use CDMA technology													
override-gateway *	Enable/disable LTE gateway override.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Override gateway to 0.0.0.0</td></tr><tr><td>disable</td><td>Use gateway as assigned by ISP DHCP server.</td></tr></table>	Option	Description	enable	Override gateway to 0.0.0.0	disable	Use gateway as assigned by ISP DHCP server.							
Option	Description													
enable	Override gateway to 0.0.0.0													
disable	Use gateway as assigned by ISP DHCP server.													
passwd	Authentication password for PDP-IP packet data calls.	password	Not Specified											
sim-hot-swap *	Enable/disable SIM card auto detection and hot swap.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable SIM card auto detection.</td></tr><tr><td>disable</td><td>Disable SIM card auto detection.</td></tr></table>	Option	Description	enable	Enable SIM card auto detection.	disable	Disable SIM card auto detection.							
Option	Description													
enable	Enable SIM card auto detection.													
disable	Disable SIM card auto detection.													
sim-slot *	SIM card slot. 1: right slot. 2: left slot.	integer	Minimum value: 1 Maximum value: 2	1										
sim1-pin *	PIN code for SIM #1 (if applicable).	password	Not Specified											
sim2-pin *	PIN code for SIM #2 (if applicable).	password	Not Specified											
status	Enable/disable USB LTE/WIMAX device.	option	-	disable **										



Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable USB LTE/WIMA device.		
	<i>disable</i>	Disable USB LTE/WIMA device.		
username	Authentication username for PDP-IP packet data calls.	string	Maximum length: 63	

\* This parameter may not exist in some models.

\*\* Values may differ between models.

## config system mac-address-table

Configure MAC address tables.

```
config system mac-address-table
    Description: Configure MAC address tables.
    edit <mac>
        set interface {string}
        set reply-substitute {mac-address}
    next
end
```

## config system mac-address-table

Parameter	Description	Type	Size	Default
interface	Interface name.	string	Maximum length: 35	
mac	MAC address.	mac-address	Not Specified	00:00:00:00:00:00
reply-substitute	New MAC for reply traffic.	mac-address	Not Specified	00:00:00:00:00:00

## config system management-tunnel

Management tunnel configuration.

```
config system management-tunnel
    Description: Management tunnel configuration.
    set allow-collect-statistics [enable|disable]
    set allow-config-restore [enable|disable]
    set allow-push-configuration [enable|disable]
    set allow-push-firmware [enable|disable]
    set authorized-manager-only [enable|disable]
    set serial-number {user}
```

```

set status [enable|disable]
end

```

## config system management-tunnel

Parameter	Description	Type	Size	Default
allow-collect-statistics	Enable/disable collection of run time statistics.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable collection of run time statistics.		
	<i>disable</i>	Disable collection of run time statistics.		
allow-config-restore	Enable/disable allow config restore.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable allow config restore.		
	<i>disable</i>	Disable allow config restore.		
allow-push-configuration	Enable/disable push configuration.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable push configuration.		
	<i>disable</i>	Disable push configuration.		
allow-push-firmware	Enable/disable push firmware.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable push firmware.		
	<i>disable</i>	Disable push firmware.		
authorized-manager-only	Enable/disable restriction of authorized manager only.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable restriction of authorized manager only.		
	<i>disable</i>	Disable restriction of authorized manager only.		
serial-number	Serial number.	user	Not Specified	

Parameter	Description	Type	Size	Default
status	Enable/disable FGFM tunnel.	option	-	enable
	Option	Description		
	<i>enable</i>	Enable management tunnel.		
	<i>disable</i>	Disable management tunnel.		

## config system mobile-tunnel

Configure Mobile tunnels, an implementation of Network Mobility (NEMO) extensions for Mobile IPv4 RFC5177.

config system mobile-tunnel

Description: Configure Mobile tunnels, an implementation of Network Mobility (NEMO) extensions for Mobile IPv4 RFC5177.

```

edit <name>
    set hash-algorithm {option}
    set home-address {ipv4-address}
    set home-agent {ipv4-address}
    set lifetime {integer}
    set n-mhae-key {password_aes256}
    set n-mhae-key-type [ascii|base64]
    set n-mhae-spi {integer}
    config network
        Description: NEMO network configuration.
        edit <id>
            set interface {string}
            set prefix {ipv4-classnet}
        next
    end
    set reg-interval {integer}
    set reg-retry {integer}
    set renew-interval {integer}
    set roaming-interface {string}
    set status [disable|enable]
    set tunnel-mode {option}
next
end

```

## config system mobile-tunnel

Parameter	Description	Type	Size	Default
hash-algorithm	Hash Algorithm (Keyed MD5).	option	-	hmac-md5
	Option	Description		
	<i>hmac-md5</i>	Keyed MD5.		

Parameter	Description	Type	Size	Default						
home-address	Home IP address (Format: xxx.xxx.xxx.xxx).	ipv4-address	Not Specified	0.0.0.0						
home-agent	IPv4 address of the NEMO HA (Format: xxx.xxx.xxx.xxx).	ipv4-address	Not Specified	0.0.0.0						
lifetime	NMMO HA registration request lifetime.	integer	Minimum value: 180 Maximum value: 65535	65535						
n-mhae-key	NEMO authentication key.	password_aes256	Not Specified							
n-mhae-key-type	NEMO authentication key type (ASCII or base64).	option	-	ascii						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ascii</td><td>The authentication key is an ASCII string.</td></tr><tr><td>base64</td><td>The authentication key is Base64 encoded.</td></tr></table>				Option	Description	ascii	The authentication key is an ASCII string.	base64	The authentication key is Base64 encoded.
Option	Description									
ascii	The authentication key is an ASCII string.									
base64	The authentication key is Base64 encoded.									
n-mhae-spi	NEMO authentication SPI.	integer	Minimum value: 0 Maximum value: 4294967295	256						
name	Tunnel name.	string	Maximum length: 15							
reg-interval	NMMO HA registration interval.	integer	Minimum value: 5 Maximum value: 300	5						
reg-retry	Maximum number of NMMO HA registration retries.	integer	Minimum value: 1 Maximum value: 30	3						
renew-interval	Time before lifetime expiration to send NMMO HA re-registration.	integer	Minimum value: 5 Maximum value: 60	60						
roaming-interface	Select the associated interface name from available options.	string	Maximum length: 15							
status	Enable/disable this mobile tunnel.	option	-	enable						

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable this mobile tunnel.		
	<i>enable</i>	Enable this mobile tunnel.		
tunnel-mode	NEMO tunnel mode (GRE tunnel).	option	-	gre
	<b>Option</b>	<b>Description</b>		
	<i>gre</i>	GRE tunnel.		

## config network

Parameter	Description	Type	Size	Default
id	Network entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
interface	Select the associated interface name from available options.	string	Maximum length: 15	
prefix	Class IP and Netmask with correction (Format:xxx.xxx.xxx.xxx xxx.xxx.xxx.xxx or xxx.xxx.xxx.xxx/x).	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0

## config system modem



This command is available for model(s): FortiGate 1000D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3900E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate VM64.

### Configure MODEM.

```
config system modem
  Description: Configure MODEM.
  set action [dial|stop|...]
  set altmode [enable|disable]
  set authtype1 {option1}, {option2}, ...
  set authtype2 {option1}, {option2}, ...
  set authtype3 {option1}, {option2}, ...
  set auto-dial [enable|disable]
  set connect-timeout {integer}
  set dial-cmd1 {string}
  set dial-cmd2 {string}
  set dial-cmd3 {string}
  set dial-on-demand [enable|disable]
  set distance {integer}
  set dont-send-CR1 [enable|disable]
  set dont-send-CR2 [enable|disable]
  set dont-send-CR3 [enable|disable]
  set extra-init1 {string}
  set extra-init2 {string}
  set extra-init3 {string}
  set holddown-timer {integer}
  set idle-timer {integer}
  set interface {string}
  set lockdown-lac {string}
  set mode [standalone|redundant]
```

```

set network-init {string}
set passwd1 {password}
set passwd2 {password}
set passwd3 {password}
set peer-modem1 [generic|actiontec|...]
set peer-modem2 [generic|actiontec|...]
set peer-modem3 [generic|actiontec|...]
set phone1 {string}
set phone2 {string}
set phone3 {string}
set pin-init {string}
set ppp-echo-request1 [enable|disable]
set ppp-echo-request2 [enable|disable]
set ppp-echo-request3 [enable|disable]
set priority {integer}
set redial [none|1|...]
set reset {integer}
set status [enable|disable]
set traffic-check [enable|disable]
set username1 {string}
set username2 {string}
set username3 {string}
set wireless-port {integer}

```

end

## config system modem

Parameter	Description	Type	Size	Default								
action	Dial up/stop MODEM.	option	-	stop								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>dial</td><td>Dial up number.</td></tr><tr><td>stop</td><td>Stop dialup.</td></tr><tr><td>none</td><td>No action.</td></tr></table>	Option	Description	dial	Dial up number.	stop	Stop dialup.	none	No action.			
	Option	Description										
	dial	Dial up number.										
	stop	Stop dialup.										
none	No action.											
altmode	Enable/disable altmode for installations using PPP in China.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>	Option	Description	enable	Enable setting.	disable	Disable setting.					
	Option	Description										
	enable	Enable setting.										
disable	Disable setting.											
authtype1	Allowed authentication types for ISP 1.	option	-	pap chap mschap mschapv2								

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>pap</i>	PAP		
	<i>chap</i>	CHAP		
	<i>mschap</i>	MSCHAP		
	<i>mschapv2</i>	MSCHAPv2		
authtype2	Allowed authentication types for ISP 2.	option	-	pap chap mschap mschapv2
	<b>Option</b>	<b>Description</b>		
	<i>pap</i>	PAP		
	<i>chap</i>	CHAP		
	<i>mschap</i>	MSCHAP		
	<i>mschapv2</i>	MSCHAPv2		
authtype3	Allowed authentication types for ISP 3.	option	-	pap chap mschap mschapv2
	<b>Option</b>	<b>Description</b>		
	<i>pap</i>	PAP		
	<i>chap</i>	CHAP		
	<i>mschap</i>	MSCHAP		
	<i>mschapv2</i>	MSCHAPv2		
auto-dial	Enable/disable auto-dial after a reboot or disconnection.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
connect-timeout	Connection completion timeout.	integer	Minimum value: 30 Maximum value: 255	90
dial-cmd1	Dial command (this is often an ATD or ATDT command).	string	Maximum length: 63	



Parameter	Description	Type	Size	Default						
dial-cmd2	Dial command (this is often an ATD or ATDT command).	string	Maximum length: 63							
dial-cmd3	Dial command (this is often an ATD or ATDT command).	string	Maximum length: 63							
dial-on-demand	Enable/disable to dial the modem when packets are routed to the modem interface.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
distance	Distance of learned routes.	integer	Minimum value: 1 Maximum value: 255	1						
dont-send-CR1	Do not send CR when connected (ISP1).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
dont-send-CR2	Do not send CR when connected (ISP2).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
dont-send-CR3	Do not send CR when connected (ISP3).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
extra-init1	Extra initialization string to ISP 1.	string	Maximum length: 127							
extra-init2	Extra initialization string to ISP 2.	string	Maximum length: 127							

Parameter	Description	Type	Size	Default								
extra-init3	Extra initialization string to ISP 3.	string	Maximum length: 127									
holddown-timer	Hold down timer in seconds.	integer	Minimum value: 1 Maximum value: 60	60								
idle-timer	MODEM connection idle time.	integer	Minimum value: 1 Maximum value: 9999	5								
interface	Name of redundant interface.	string	Maximum length: 63									
lockdown-lac	Allow connection only to the specified Location Area Code (LAC).	string	Maximum length: 127									
mode	Set MODEM operation mode to redundant or standalone.	option	-	standalone								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>standalone</i></td><td>Standalone.</td></tr><tr><td><i>redundant</i></td><td>Redundant for an interface.</td></tr></table>				Option	Description	<i>standalone</i>	Standalone.	<i>redundant</i>	Redundant for an interface.		
Option	Description											
<i>standalone</i>	Standalone.											
<i>redundant</i>	Redundant for an interface.											
network-init	AT command to set the Network name/type (AT+COPS=<mode>,[<format>,<oper>[,<AcT>]]).	string	Maximum length: 127									
passwd1	Password to access the specified dialup account.	password	Not Specified									
passwd2	Password to access the specified dialup account.	password	Not Specified									
passwd3	Password to access the specified dialup account.	password	Not Specified									
peer-modem1	Specify peer MODEM type for phone1.	option	-	generic								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>generic</i></td><td>All other modem type.</td></tr><tr><td><i>actiontec</i></td><td>ActionTec modem.</td></tr><tr><td><i>ascend_TNT</i></td><td>Ascend TNT modem.</td></tr></table>				Option	Description	<i>generic</i>	All other modem type.	<i>actiontec</i>	ActionTec modem.	<i>ascend_TNT</i>	Ascend TNT modem.
Option	Description											
<i>generic</i>	All other modem type.											
<i>actiontec</i>	ActionTec modem.											
<i>ascend_TNT</i>	Ascend TNT modem.											
peer-modem2	Specify peer MODEM type for phone2.	option	-	generic								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>generic</i></td><td>All other modem type.</td></tr></table>				Option	Description	<i>generic</i>	All other modem type.				
Option	Description											
<i>generic</i>	All other modem type.											

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>actiontec</i>	ActionTec modem.		
	<i>ascend_TNT</i>	Ascend TNT modem.		
peer-modem3	Specify peer MODEM type for phone3.	option	-	generic
	<b>Option</b>	<b>Description</b>		
	<i>generic</i>	All other modem type.		
	<i>actiontec</i>	ActionTec modem.		
	<i>ascend_TNT</i>	Ascend TNT modem.		
phone1	Phone number to connect to the dialup account (must not contain spaces, and should include standard special characters).	string	Maximum length: 63	
phone2	Phone number to connect to the dialup account (must not contain spaces, and should include standard special characters).	string	Maximum length: 63	
phone3	Phone number to connect to the dialup account (must not contain spaces, and should include standard special characters).	string	Maximum length: 63	
pin-init	AT command to set the PIN (AT+PIN=<pin>).	string	Maximum length: 127	
ppp-echo-request1	Enable/disable PPP echo-request to ISP 1.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
ppp-echo-request2	Enable/disable PPP echo-request to ISP 2.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
ppp-echo-request3	Enable/disable PPP echo-request to ISP 3.	option	-	enable

Parameter	Description	Type	Size	Default																								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.																					
	Option	Description																										
	<i>enable</i>	Enable setting.																										
<i>disable</i>	Disable setting.																											
priority	Priority of learned routes.	integer	Minimum value: 0 Maximum value: 4294967295	0																								
redial	Redial limit.	option	-	none																								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>Forever.</td></tr><tr><td><i>1</i></td><td>One attempt.</td></tr><tr><td><i>2</i></td><td>Two attempts.</td></tr><tr><td><i>3</i></td><td>Three attempts.</td></tr><tr><td><i>4</i></td><td>Four attempts.</td></tr><tr><td><i>5</i></td><td>Five attempts.</td></tr><tr><td><i>6</i></td><td>Six attempts.</td></tr><tr><td><i>7</i></td><td>Seven attempts.</td></tr><tr><td><i>8</i></td><td>Eight attempts.</td></tr><tr><td><i>9</i></td><td>Nine attempts.</td></tr><tr><td><i>10</i></td><td>Ten attempts.</td></tr></table>	Option	Description	<i>none</i>	Forever.	<i>1</i>	One attempt.	<i>2</i>	Two attempts.	<i>3</i>	Three attempts.	<i>4</i>	Four attempts.	<i>5</i>	Five attempts.	<i>6</i>	Six attempts.	<i>7</i>	Seven attempts.	<i>8</i>	Eight attempts.	<i>9</i>	Nine attempts.	<i>10</i>	Ten attempts.			
	Option	Description																										
	<i>none</i>	Forever.																										
	<i>1</i>	One attempt.																										
	<i>2</i>	Two attempts.																										
	<i>3</i>	Three attempts.																										
	<i>4</i>	Four attempts.																										
	<i>5</i>	Five attempts.																										
	<i>6</i>	Six attempts.																										
	<i>7</i>	Seven attempts.																										
	<i>8</i>	Eight attempts.																										
	<i>9</i>	Nine attempts.																										
<i>10</i>	Ten attempts.																											
reset	Number of dial attempts before resetting modem (0 = never reset).	integer	Minimum value: 0 Maximum value: 10	0																								
status	Enable/disable Modem support (equivalent to bringing an interface up or down).	option	-	disable																								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.																					
	Option	Description																										
	<i>enable</i>	Enable setting.																										
<i>disable</i>	Disable setting.																											
traffic-check	Enable/disable traffic-check.	option	-	disable																								

Parameter	Description	Type	Size	Default
	Option Description			
	<i>enable</i>			
	<i>disable</i>			
username1	User name to access the specified dialup account.	string	Maximum length: 63	
username2	User name to access the specified dialup account.	string	Maximum length: 63	
username3	User name to access the specified dialup account.	string	Maximum length: 63	
wireless-port	Enter wireless port number, 0 for default, 1 for first port, ...	integer	Minimum value: 0 Maximum value: 4294967295	0

## config system nd-proxy

Configure IPv6 neighbor discovery proxy (RFC4389).

```
config system nd-proxy
    Description: Configure IPv6 neighbor discovery proxy (RFC4389).
    set member <interface-name1>, <interface-name2>, ...
    set status [enable|disable]
end
```

## config system nd-proxy

Parameter	Description	Type	Size	Default
member <interface-name>	Interfaces using the neighbor discovery proxy. Interface name.	string	Maximum length: 79	
status	Enable/disable neighbor discovery proxy.	option	-	disable
	Option Description			
	<i>enable</i>			
	<i>disable</i>			

## config system netflow

Configure NetFlow.

```
config system netflow
  Description: Configure NetFlow.
  set active-flow-timeout {integer}
  set collector-ip {ipv4-address}
  set collector-port {integer}
  set inactive-flow-timeout {integer}
  set interface {string}
  set interface-select-method [auto|sdwan|...]
  set source-ip {ipv4-address}
  set template-tx-counter {integer}
  set template-tx-timeout {integer}
end
```

## config system netflow

Parameter	Description	Type	Size	Default
active-flow-timeout	Timeout to report active flows.	integer	Minimum value: 60 Maximum value: 3600	1800
collector-ip	Collector IP.	ipv4-address	Not Specified	0.0.0.0
collector-port	NetFlow collector port number.	integer	Minimum value: 0 Maximum value: 65535	2055
inactive-flow-timeout	Timeout for periodic report of finished flows.	integer	Minimum value: 10 Maximum value: 600	15
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto
		Option	Description	
		auto	Set outgoing interface automatically.	
		sdwan	Set outgoing interface by SD-WAN or policy routing rules.	
		specify	Set outgoing interface manually.	

Parameter	Description	Type	Size	Default
source-ip	Source IP address for communication with the NetFlow agent.	ipv4-address	Not Specified	0.0.0.0
template-tx-counter	Counter of flowset records before resending a template flowset record.	integer	Minimum value: 10 Maximum value: 6000	20
template-tx-timeout	Timeout for periodic template flowset transmission.	integer	Minimum value: 60 Maximum value: 86400	1800

## config system network-visibility

Configure network visibility settings.

```
config system network-visibility
    Description: Configure network visibility settings.
    set destination-hostname-visibility [disable|enable]
    set destination-location [disable|enable]
    set destination-visibility [disable|enable]
    set hostname-limit {integer}
    set hostname-ttl {integer}
    set source-location [disable|enable]
end
```

## config system network-visibility

Parameter	Description	Type	Size	Default
destination-hostname-visibility	Enable/disable logging of destination hostname visibility.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable logging of destination hostname visibility.		
	<i>enable</i>	Enable logging of destination hostname visibility.		
destination-location	Enable/disable logging of destination geographical location visibility.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable logging of destination geographical location visibility.		
	<i>enable</i>	Enable logging of destination geographical location visibility.		

Parameter	Description	Type	Size	Default						
destination-visibility	Enable/disable logging of destination visibility.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable logging of destination visibility.</td></tr><tr><td><i>enable</i></td><td>Enable logging of destination visibility.</td></tr></table>	Option	Description	<i>disable</i>	Disable logging of destination visibility.	<i>enable</i>	Enable logging of destination visibility.			
Option	Description									
<i>disable</i>	Disable logging of destination visibility.									
<i>enable</i>	Enable logging of destination visibility.									
hostname-limit	Limit of the number of hostname table entries.	integer	Minimum value: 0 Maximum value: 50000	5000						
hostname-ttl	TTL of hostname table entries.	integer	Minimum value: 60 Maximum value: 86400	86400						
source-location	Enable/disable logging of source geographical location visibility.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable logging of source geographical location visibility.</td></tr><tr><td><i>enable</i></td><td>Enable logging of source geographical location visibility.</td></tr></table>	Option	Description	<i>disable</i>	Disable logging of source geographical location visibility.	<i>enable</i>	Enable logging of source geographical location visibility.			
Option	Description									
<i>disable</i>	Disable logging of source geographical location visibility.									
<i>enable</i>	Enable logging of source geographical location visibility.									



## config system np6



This command is available for model(s): FortiGate 1000D, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 1500DT, FortiGate 1500D, FortiGate 2000E, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 3000D, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 401E, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 601E, FortiGate 800D, FortiGate 900D.

It is not available for: FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 140E-POE, FortiGate 140E, FortiGate 1800F, FortiGate 1801F, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2600F, FortiGate 2601F, FortiGate 3000F, FortiGate 3001F, FortiGate 3500F, FortiGate 3501F, FortiGate 400F, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 600F, FortiGate 601F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 90E, FortiGate 91E, FortiGate VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

### Configure NP6 attributes.

```
config system np6
  Description: Configure NP6 attributes.
  edit <name>
    set fastpath [disable|enable]
    config fp-anomaly
      Description: NP6 IPv4 anomaly protection. trap-to-host forwards anomaly sessions
to the CPU.
      set tcp-syn-fin [allow|drop|...]
      set tcp-fin-noack [allow|drop|...]
      set tcp-fin-only [allow|drop|...]
      set tcp-no-flag [allow|drop|...]
      set tcp-syn-data [allow|drop|...]
      set tcp-winnuke [allow|drop|...]
      set tcp-land [allow|drop|...]
      set udp-land [allow|drop|...]
      set icmp-land [allow|drop|...]
      set icmp-frag [allow|drop|...]
      set ipv4-land [allow|drop|...]
      set ipv4-proto-err [allow|drop|...]
      set ipv4-unknopt [allow|drop|...]
      set ipv4-optrr [allow|drop|...]
      set ipv4-optssrr [allow|drop|...]
      set ipv4-optlsrr [allow|drop|...]
      set ipv4-optstream [allow|drop|...]
      set ipv4-optsecurity [allow|drop|...]
```

```

        set ipv4-opttimestamp [allow|drop|...]
        set ipv4-csum-err [drop|trap-to-host]
        set tcp-csum-err [drop|trap-to-host]
        set udp-csum-err [drop|trap-to-host]
        set icmp-csum-err [drop|trap-to-host]
        set ipv6-land [allow|drop|...]
        set ipv6-proto-err [allow|drop|...]
        set ipv6-unknopt [allow|drop|...]
        set ipv6-saddr-err [allow|drop|...]
        set ipv6-daddr-err [allow|drop|...]
        set ipv6-optralert [allow|drop|...]
        set ipv6-optjumbo [allow|drop|...]
        set ipv6-opttunnel [allow|drop|...]
        set ipv6-opthomeaddr [allow|drop|...]
        set ipv6-optnsap [allow|drop|...]
        set ipv6-optendpid [allow|drop|...]
        set ipv6-optinvld [allow|drop|...]
    end
    set garbage-session-collector [disable|enable]
    config hpe
        Description: HPE configuration.
        set tcpsyn-max {integer}
        set tcpsyn-ack-max {integer}
        set tcpfin-rst-max {integer}
        set tcp-max {integer}
        set udp-max {integer}
        set icmp-max {integer}
        set sctp-max {integer}
        set esp-max {integer}
        set ip-frag-max {integer}
        set ip-others-max {integer}
        set arp-max {integer}
        set l2-others-max {integer}
        set pri-type-max {integer}
        set enable-shaper [disable|enable]
    end
    set ipsec-ob-hash-function [switch-group-hash|global-hash|...]
    set ipsec-outbound-hash [disable|enable]
    set low-latency-mode [disable|enable]
    set per-session-accounting [disable|traffic-log-only|...]
    set session-collector-interval {integer}
    set session-timeout-fixed [disable|enable]
    set session-timeout-interval {integer}
    set session-timeout-random-range {integer}
next
end

```

## config system np6

Parameter	Description	Type	Size	Default
fastpath	Enable/disable NP4 or NP6 offloading (also called fast path).	option	-	enable

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable NP4 or NP6 offloading (fast path).		
	<i>enable</i>	Enable NP4 or NP6 offloading (fast path).		
garbage-session-collector	Enable/disable garbage session collector.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable garbage session collector.		
	<i>enable</i>	Enable garbage session collector.		
ipsec-ob-hash-function *	Set hash function for IPsec outbound.	option	-	switch-group-hash
	<b>Option</b>	<b>Description</b>		
	<i>switch-group-hash</i>	Hash outbound SA traffic within NPs connected to same switch.		
	<i>global-hash</i>	Hash outbound SA traffic among all NPs.		
	<i>global-hash-weighted</i>	Hash outbound SA traffic among all NPs with more weights on NPs connected to switch 0. It's applicable to the case that ingress traffic is from switch 1.		
	<i>round-robin-switch-group</i>	Round-robin outbound SA traffic within NPs connected to same switch.		
	<i>round-robin-global</i>	Round-robin outbound SA traffic among all NPs.		
ipsec-outbound-hash *	Enable/disable hash function for IPsec outbound traffic.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable hash function for IPsec outbound traffic.		
	<i>enable</i>	Enable hash function for IPsec outbound traffic.		
low-latency-mode	Enable/disable low latency mode.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable low latency mode.		

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable low latency mode.</td></tr></table>				Option	Description	<i>enable</i>	Enable low latency mode.				
	Option	Description										
<i>enable</i>	Enable low latency mode.											
name	Device Name.	string	Maximum length: 31									
per-session-accounting	Enable/disable per-session accounting.	option	-	traffic-log-only								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable per-session accounting.</td></tr><tr><td><i>traffic-log-only</i></td><td>Per-session accounting only for sessions with traffic logging enabled in firewall policy.</td></tr><tr><td><i>enable</i></td><td>Per-session accounting for all sessions.</td></tr></table>				Option	Description	<i>disable</i>	Disable per-session accounting.	<i>traffic-log-only</i>	Per-session accounting only for sessions with traffic logging enabled in firewall policy.	<i>enable</i>	Per-session accounting for all sessions.
	Option	Description										
	<i>disable</i>	Disable per-session accounting.										
	<i>traffic-log-only</i>	Per-session accounting only for sessions with traffic logging enabled in firewall policy.										
<i>enable</i>	Per-session accounting for all sessions.											
session-collector-interval	Set garbage session collection cleanup interval.	integer	Minimum value: 1 Maximum value: 100	64								
session-timeout-fixed	{disable   enable} Toggle between using fixed or random timeouts for refreshing NP6 sessions.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable Refresh NP6 sessions at the configured fixed interval.</td></tr><tr><td><i>enable</i></td><td>Enable Refresh NP6 sessions randomly where the time between refreshes is within the random range.</td></tr></table>				Option	Description	<i>disable</i>	Disable Refresh NP6 sessions at the configured fixed interval.	<i>enable</i>	Enable Refresh NP6 sessions randomly where the time between refreshes is within the random range.		
	Option	Description										
	<i>disable</i>	Disable Refresh NP6 sessions at the configured fixed interval.										
<i>enable</i>	Enable Refresh NP6 sessions randomly where the time between refreshes is within the random range.											
session-timeout-interval	Set the fixed timeout for refreshing NP6 sessions.	integer	Minimum value: 0 Maximum value: 1000	40								
session-timeout-random-range	Set the random timeout range for refreshing NP6 sessions.	integer	Minimum value: 0 Maximum value: 1000	8								

\* This parameter may not exist in some models.

### config fp-anomaly

Parameter	Description	Type	Size	Default
tcp-syn-fin	TCP SYN flood SYN/FIN flag set anomalies.	option	-	allow

Parameter	Description	Type	Size	Default
	<b>Option</b> <b>Description</b>			
	<i>allow</i>	Allow TCP packets with syn_fin flag set to pass.		
	<i>drop</i>	Drop TCP packets with syn_fin flag set.		
	<i>trap-to-host</i>	Forward TCP packets with syn_fin flag set to FortiOS.		
tcp-fin-noack	TCP SYN flood with FIN flag set without ACK setting anomalies.	option	-	trap-to-host
	<b>Option</b> <b>Description</b>			
	<i>allow</i>	Allow TCP packets with FIN flag set without ack setting to pass.		
	<i>drop</i>	Drop TCP packets with FIN flag set without ack setting.		
	<i>trap-to-host</i>	Forward TCP packets with FIN flag set without ack setting to FortiOS.		
tcp-fin-only	TCP SYN flood with only FIN flag set anomalies.	option	-	trap-to-host
	<b>Option</b> <b>Description</b>			
	<i>allow</i>	Allow TCP packets with FIN flag set only to pass.		
	<i>drop</i>	Drop TCP packets with FIN flag set only.		
	<i>trap-to-host</i>	Forward TCP packets with FIN flag set only to FortiOS.		
tcp-no-flag	TCP SYN flood with no flag set anomalies.	option	-	allow
	<b>Option</b> <b>Description</b>			
	<i>allow</i>	Allow TCP packets without flag set to pass.		
	<i>drop</i>	Drop TCP packets without flag set.		
	<i>trap-to-host</i>	Forward TCP packets without flag set to FortiOS.		
tcp-syn-data	TCP SYN flood packets with data anomalies.	option	-	allow
	<b>Option</b> <b>Description</b>			
	<i>allow</i>	Allow TCP syn packets with data to pass.		
	<i>drop</i>	Drop TCP syn packets with data.		
	<i>trap-to-host</i>	Forward TCP syn packets with data to FortiOS.		
tcp-winnuke	TCP WinNuke anomalies.	option	-	trap-to-host
	<b>Option</b> <b>Description</b>			
	<i>allow</i>	Allow TCP packets winnuke attack to pass.		

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>drop</td><td>Drop TCP packets winnuke attack.</td></tr><tr><td>trap-to-host</td><td>Forward TCP packets winnuke attack to FortiOS.</td></tr></table>	Option	Description	drop	Drop TCP packets winnuke attack.	trap-to-host	Forward TCP packets winnuke attack to FortiOS.					
	Option	Description										
	drop	Drop TCP packets winnuke attack.										
	trap-to-host	Forward TCP packets winnuke attack to FortiOS.										
tcp-land	TCP land anomalies.	option	-	trap-to-host								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allow TCP land attack to pass.</td></tr><tr><td>drop</td><td>Drop TCP land attack.</td></tr><tr><td>trap-to-host</td><td>Forward TCP land attack to FortiOS.</td></tr></table>	Option	Description	allow	Allow TCP land attack to pass.	drop	Drop TCP land attack.	trap-to-host	Forward TCP land attack to FortiOS.			
	Option	Description										
	allow	Allow TCP land attack to pass.										
	drop	Drop TCP land attack.										
trap-to-host	Forward TCP land attack to FortiOS.											
udp-land	UDP land anomalies.	option	-	trap-to-host								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allow UDP land attack to pass.</td></tr><tr><td>drop</td><td>Drop UDP land attack.</td></tr><tr><td>trap-to-host</td><td>Forward UDP land attack to FortiOS.</td></tr></table>	Option	Description	allow	Allow UDP land attack to pass.	drop	Drop UDP land attack.	trap-to-host	Forward UDP land attack to FortiOS.			
	Option	Description										
	allow	Allow UDP land attack to pass.										
	drop	Drop UDP land attack.										
trap-to-host	Forward UDP land attack to FortiOS.											
icmp-land	ICMP land anomalies.	option	-	trap-to-host								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allow ICMP land attack to pass.</td></tr><tr><td>drop</td><td>Drop ICMP land attack.</td></tr><tr><td>trap-to-host</td><td>Forward ICMP land attack to FortiOS.</td></tr></table>	Option	Description	allow	Allow ICMP land attack to pass.	drop	Drop ICMP land attack.	trap-to-host	Forward ICMP land attack to FortiOS.			
	Option	Description										
	allow	Allow ICMP land attack to pass.										
	drop	Drop ICMP land attack.										
trap-to-host	Forward ICMP land attack to FortiOS.											
icmp-frag	Layer 3 fragmented packets that could be part of layer 4 ICMP anomalies.	option	-	allow								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allow L3 fragment packet with L4 protocol as ICMP attack to pass.</td></tr><tr><td>drop</td><td>Drop L3 fragment packet with L4 protocol as ICMP attack.</td></tr><tr><td>trap-to-host</td><td>Forward L3 fragment packet with L4 protocol as ICMP attack to FortiOS.</td></tr></table>	Option	Description	allow	Allow L3 fragment packet with L4 protocol as ICMP attack to pass.	drop	Drop L3 fragment packet with L4 protocol as ICMP attack.	trap-to-host	Forward L3 fragment packet with L4 protocol as ICMP attack to FortiOS.			
	Option	Description										
	allow	Allow L3 fragment packet with L4 protocol as ICMP attack to pass.										
	drop	Drop L3 fragment packet with L4 protocol as ICMP attack.										
trap-to-host	Forward L3 fragment packet with L4 protocol as ICMP attack to FortiOS.											
ipv4-land	Land anomalies.	option	-	trap-to-host								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allow IPv4 land attack to pass.</td></tr><tr><td>drop</td><td>Drop IPv4 land attack.</td></tr></table>	Option	Description	allow	Allow IPv4 land attack to pass.	drop	Drop IPv4 land attack.					
	Option	Description										
	allow	Allow IPv4 land attack to pass.										
drop	Drop IPv4 land attack.											

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>trap-to-host</td><td>Forward IPv4 land attack to FortiOS.</td></tr></table>	Option	Description	trap-to-host	Forward IPv4 land attack to FortiOS.							
	Option	Description										
	trap-to-host	Forward IPv4 land attack to FortiOS.										
ipv4-proto-err	Invalid layer 4 protocol anomalies.	option	-	trap-to-host								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allow IPv4 invalid L4 protocol to pass.</td></tr><tr><td>drop</td><td>Drop IPv4 invalid L4 protocol.</td></tr><tr><td>trap-to-host</td><td>Forward IPv4 invalid L4 protocol to FortiOS.</td></tr></table>	Option	Description	allow	Allow IPv4 invalid L4 protocol to pass.	drop	Drop IPv4 invalid L4 protocol.	trap-to-host	Forward IPv4 invalid L4 protocol to FortiOS.			
	Option	Description										
	allow	Allow IPv4 invalid L4 protocol to pass.										
	drop	Drop IPv4 invalid L4 protocol.										
trap-to-host	Forward IPv4 invalid L4 protocol to FortiOS.											
ipv4-unknopt	Unknown option anomalies.	option	-	trap-to-host								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allow IPv4 with unknown options to pass.</td></tr><tr><td>drop</td><td>Drop IPv4 with unknown options.</td></tr><tr><td>trap-to-host</td><td>Forward IPv4 with unknown options to FortiOS.</td></tr></table>	Option	Description	allow	Allow IPv4 with unknown options to pass.	drop	Drop IPv4 with unknown options.	trap-to-host	Forward IPv4 with unknown options to FortiOS.			
	Option	Description										
	allow	Allow IPv4 with unknown options to pass.										
	drop	Drop IPv4 with unknown options.										
trap-to-host	Forward IPv4 with unknown options to FortiOS.											
ipv4-optrr	Record route option anomalies.	option	-	trap-to-host								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allow IPv4 with record route option to pass.</td></tr><tr><td>drop</td><td>Drop IPv4 with record route option.</td></tr><tr><td>trap-to-host</td><td>Forward IPv4 with record route option to FortiOS.</td></tr></table>	Option	Description	allow	Allow IPv4 with record route option to pass.	drop	Drop IPv4 with record route option.	trap-to-host	Forward IPv4 with record route option to FortiOS.			
	Option	Description										
	allow	Allow IPv4 with record route option to pass.										
	drop	Drop IPv4 with record route option.										
trap-to-host	Forward IPv4 with record route option to FortiOS.											
ipv4-optssrr	Strict source record route option anomalies.	option	-	trap-to-host								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allow IPv4 with strict source record route option to pass.</td></tr><tr><td>drop</td><td>Drop IPv4 with strict source record route option.</td></tr><tr><td>trap-to-host</td><td>Forward IPv4 with strict source record route option to FortiOS.</td></tr></table>	Option	Description	allow	Allow IPv4 with strict source record route option to pass.	drop	Drop IPv4 with strict source record route option.	trap-to-host	Forward IPv4 with strict source record route option to FortiOS.			
	Option	Description										
	allow	Allow IPv4 with strict source record route option to pass.										
	drop	Drop IPv4 with strict source record route option.										
trap-to-host	Forward IPv4 with strict source record route option to FortiOS.											
ipv4-optlsrr	Loose source record route option anomalies.	option	-	trap-to-host								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allow IPv4 with loose source record route option to pass.</td></tr><tr><td>drop</td><td>Drop IPv4 with loose source record route option.</td></tr><tr><td>trap-to-host</td><td>Forward IPv4 with loose source record route option to FortiOS.</td></tr></table>	Option	Description	allow	Allow IPv4 with loose source record route option to pass.	drop	Drop IPv4 with loose source record route option.	trap-to-host	Forward IPv4 with loose source record route option to FortiOS.			
	Option	Description										
	allow	Allow IPv4 with loose source record route option to pass.										
	drop	Drop IPv4 with loose source record route option.										
trap-to-host	Forward IPv4 with loose source record route option to FortiOS.											
ipv4-optstream	Stream option anomalies.	option	-	trap-to-host								

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow IPv4 with stream option to pass.		
	<i>drop</i>	Drop IPv4 with stream option.		
	<i>trap-to-host</i>	Forward IPv4 with stream option to FortiOS.		
ipv4-optsecurity	Security option anomalies.	option	-	trap-to-host
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow IPv4 with security option to pass.		
	<i>drop</i>	Drop IPv4 with security option.		
	<i>trap-to-host</i>	Forward IPv4 with security option to FortiOS.		
ipv4-opttimestamp	Timestamp option anomalies.	option	-	trap-to-host
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow IPv4 with timestamp option to pass.		
	<i>drop</i>	Drop IPv4 with timestamp option.		
	<i>trap-to-host</i>	Forward IPv4 with timestamp option to FortiOS.		
ipv4-csum-err	Invalid IPv4 IP checksum anomalies.	option	-	drop
	<b>Option</b>	<b>Description</b>		
	<i>drop</i>	Drop IPv4 invalid IP checksum.		
	<i>trap-to-host</i>	Forward IPv4 invalid IP checksum to main CPU for processing.		
tcp-csum-err	Invalid IPv4 TCP checksum anomalies.	option	-	drop
	<b>Option</b>	<b>Description</b>		
	<i>drop</i>	Drop IPv4 invalid TCP checksum.		
	<i>trap-to-host</i>	Forward IPv4 invalid TCP checksum to main CPU for processing.		
udp-csum-err	Invalid IPv4 UDP checksum anomalies.	option	-	drop
	<b>Option</b>	<b>Description</b>		
	<i>drop</i>	Drop IPv4 invalid UDP checksum.		
	<i>trap-to-host</i>	Forward IPv4 invalid UDP checksum to main CPU for processing.		
icmp-csum-err	Invalid IPv4 ICMP checksum anomalies.	option	-	drop



Parameter	Description	Type	Size	Default
	Option	Description		
	drop	Drop IPv4 invalid ICMP checksum.		
	trap-to-host	Forward IPv4 invalid ICMP checksum to main CPU for processing.		
ipv6-land	Land anomalies.	option	-	trap-to-host
	Option	Description		
	allow	Allow IPv6 land attack to pass.		
	drop	Drop IPv6 land attack.		
	trap-to-host	Forward IPv6 land attack to FortiOS.		
ipv6-proto-err	Layer 4 invalid protocol anomalies.	option	-	trap-to-host
	Option	Description		
	allow	Allow IPv6 L4 invalid protocol to pass.		
	drop	Drop IPv6 L4 invalid protocol.		
	trap-to-host	Forward IPv6 L4 invalid protocol to FortiOS.		
ipv6-unknpt	Unknown option anomalies.	option	-	trap-to-host
	Option	Description		
	allow	Allow IPv6 with unknown options to pass.		
	drop	Drop IPv6 with unknown options.		
	trap-to-host	Forward IPv6 with unknown options to FortiOS.		
ipv6-saddr-err	Source address as multicast anomalies.	option	-	trap-to-host
	Option	Description		
	allow	Allow IPv6 with source address as multicast to pass.		
	drop	Drop IPv6 with source address as multicast.		
	trap-to-host	Forward IPv6 with source address as multicast to FortiOS.		
ipv6-daddr-err	Destination address as unspecified or loopback address anomalies.	option	-	trap-to-host
	Option	Description		
	allow	Allow IPv6 with destination address as unspecified or loopback address to pass.		

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>drop</i>	Drop IPv6 with destination address as unspecified or loopback address.		
	<i>trap-to-host</i>	Forward IPv6 with destination address as unspecified or loopback address to FortiOS.		
ipv6-optralert	Router alert option anomalies.	option	-	trap-to-host
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow IPv6 with router alert option to pass.		
	<i>drop</i>	Drop IPv6 with router alert option.		
	<i>trap-to-host</i>	Forward IPv6 with router alert option to FortiOS.		
ipv6-optjumbo	Jumbo options anomalies.	option	-	trap-to-host
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow IPv6 with jumbo option to pass.		
	<i>drop</i>	Drop IPv6 with jumbo option.		
	<i>trap-to-host</i>	Forward IPv6 with jumbo option to FortiOS.		
ipv6-opttunnel	Tunnel encapsulation limit option anomalies.	option	-	trap-to-host
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow IPv6 with tunnel encapsulation limit to pass.		
	<i>drop</i>	Drop IPv6 with tunnel encapsulation limit.		
	<i>trap-to-host</i>	Forward IPv6 with tunnel encapsulation limit to FortiOS.		
ipv6-opthomeaddr	Home address option anomalies.	option	-	trap-to-host
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow IPv6 with home address option to pass.		
	<i>drop</i>	Drop IPv6 with home address option.		
	<i>trap-to-host</i>	Forward IPv6 with home address option to FortiOS.		
ipv6-optnsap	Network service access point address option anomalies.	option	-	trap-to-host

Parameter	Description	Type	Size	Default
	Option	Description		
	allow	Allow IPv6 with network service access point address option to pass.		
	drop	Drop IPv6 with network service access point address option.		
	trap-to-host	Forward IPv6 with network service access point address option to FortiOS.		
ipv6-optendpid	End point identification anomalies.	option	-	trap-to-host
	Option	Description		
	allow	Allow IPv6 with end point identification option to pass.		
	drop	Drop IPv6 with end point identification option.		
	trap-to-host	Forward IPv6 with end point identification option to FortiOS.		
ipv6-optinvld	Invalid option anomalies.Invalid option anomalies.	option	-	trap-to-host
	Option	Description		
	allow	Allow IPv6 with invalid option to pass.		
	drop	Drop IPv6 with invalid option.		
	trap-to-host	Forward IPv6 with invalid option to FortiOS.		

## config hpe

Parameter	Description	Type	Size	Default
tcpsyn-max	Maximum TCP SYN packet rate.	integer	Minimum value: 1000 Maximum value: 1000000000	600000
tcpsyn-ack-max	Maximum TCP carries SYN and ACK flags packet rate.	integer	Minimum value: 1000 Maximum value: 1000000000	600000
tcpfin-rst-max	Maximum TCP carries FIN or RST flags packet rate.	integer	Minimum value: 1000 Maximum value: 1000000000	600000

Parameter	Description	Type	Size	Default
tcp-max	Maximum TCP packet rate.	integer	Minimum value: 1000 Maximum value: 1000000000	600000
udp-max	Maximum UDP packet rate.	integer	Minimum value: 1000 Maximum value: 1000000000	600000
icmp-max	Maximum ICMP packet rate.	integer	Minimum value: 1000 Maximum value: 1000000000	200000
sctp-max	Maximum SCTP packet rate.	integer	Minimum value: 1000 Maximum value: 1000000000	200000
esp-max	Maximum ESP packet rate.	integer	Minimum value: 1000 Maximum value: 1000000000	200000
ip-frag-max	Maximum fragmented IP packet rate.	integer	Minimum value: 1000 Maximum value: 1000000000	200000
ip-others-max	Maximum IP packet rate for other packets.	integer	Minimum value: 1000 Maximum value: 1000000000	200000
arp-max	Maximum ARP packet rate.	integer	Minimum value: 1000 Maximum value: 1000000000	200000

Parameter	Description	Type	Size	Default						
l2-others-max	Maximum L2 packet rate for L2 packets that are not ARP packets.	integer	Minimum value: 1000 Maximum value: 1000000000	200000						
pri-type-max	Maximum overflow rate of priority type traffic. Includes L2: HA, 802.3ad LACP, heartbeats. L3: OSPF. L4_TCP: BGP. L4_UDP: IKE, SLBC, BFD.	integer	Minimum value: 1000 Maximum value: 1000000000	200000						
enable-shaper	Enable/Disable NPU Host Protection Engine(HPE) for packet type shaper.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable NPU HPE shaping based on packet type.</td></tr><tr><td>enable</td><td>Enable NPU HPE shaping based on packet type.</td></tr></table>				Option	Description	disable	Disable NPU HPE shaping based on packet type.	enable	Enable NPU HPE shaping based on packet type.
	Option	Description								
	disable	Disable NPU HPE shaping based on packet type.								
enable	Enable NPU HPE shaping based on packet type.									

## config system np6xlite



This command is available for model(s): FortiGate 100F, FortiGate 101F, FortiGate 200F, FortiGate 201F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81F-POE, FortiGate 81F, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60F, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 1000D, FortiGate 100EF, FortiGate 100E, FortiGate 101E, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 201E, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 61E, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 81E-POE, FortiGate 81E, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate VM64, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 61E.

Configure NP6XLITE attributes.

```

config system np6xlite
    Description: Configure NP6XLITE attributes.
    edit <name>
        set fastpath [disable|enable]
        config fp-anomaly
            Description: NP6XLITE IPv4 anomaly protection. trap-to-host forwards anomaly
sessions to the CPU.
            set tcp-syn-fin [allow|drop|...]
            set tcp-fin-noack [allow|drop|...]
            set tcp-fin-only [allow|drop|...]
            set tcp-no-flag [allow|drop|...]
            set tcp-syn-data [allow|drop|...]
            set tcp-winnuke [allow|drop|...]
            set tcp-land [allow|drop|...]
            set udp-land [allow|drop|...]
            set icmp-land [allow|drop|...]
            set icmp-frag [allow|drop|...]
            set ipv4-land [allow|drop|...]
            set ipv4-proto-err [allow|drop|...]
            set ipv4-unknopt [allow|drop|...]
            set ipv4-optrr [allow|drop|...]
            set ipv4-optssrr [allow|drop|...]
            set ipv4-optlsrr [allow|drop|...]
            set ipv4-optstream [allow|drop|...]
            set ipv4-optsecurity [allow|drop|...]
            set ipv4-opttimestamp [allow|drop|...]
            set ipv4-csum-err [drop|trap-to-host]
            set tcp-csum-err [drop|trap-to-host]
            set udp-csum-err [drop|trap-to-host]
            set icmp-csum-err [drop|trap-to-host]
            set ipv6-land [allow|drop|...]
            set ipv6-proto-err [allow|drop|...]
            set ipv6-unknopt [allow|drop|...]
            set ipv6-saddr-err [allow|drop|...]
            set ipv6-daddr-err [allow|drop|...]
            set ipv6-optralert [allow|drop|...]
            set ipv6-optjumbo [allow|drop|...]
            set ipv6-opttunnel [allow|drop|...]
            set ipv6-opthomeaddr [allow|drop|...]
            set ipv6-optnsap [allow|drop|...]
            set ipv6-optendpid [allow|drop|...]
            set ipv6-optinvld [allow|drop|...]
        end
        set garbage-session-collector [disable|enable]
    config hpe
        Description: HPE configuration.
        set tcpsyn-max {integer}
        set tcp-max {integer}
        set udp-max {integer}
        set icmp-max {integer}
        set sctp-max {integer}
        set esp-max {integer}
        set ip-frag-max {integer}
        set ip-others-max {integer}
        set arp-max {integer}
        set l2-others-max {integer}

```

```

        set enable-shaper [disable|enable]
    end
    set ipsec-STs-timeout [1|2|...]
    set ipsec-inner-fragment [disable|enable]
    set ipsec-throughput-msg-frequency [disable|32KB|...]
    set per-session-accounting [disable|traffic-log-only|...]
    set session-collector-interval {integer}
    set session-timeout-fixed [disable|enable]
    set session-timeout-interval {integer}
    set session-timeout-random-range {integer}
next
end

```

## config system np6xlite

Parameter	Description	Type	Size	Default														
fastpath	Enable/disable NP4 or NP6XLITE offloading (also called fast path).	option	-	enable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable NP4 or NP6XLITE offloading (fast path).</td></tr><tr><td><i>enable</i></td><td>Enable NP4 or NP6XLITE offloading (fast path).</td></tr></table>	Option	Description	<i>disable</i>	Disable NP4 or NP6XLITE offloading (fast path).	<i>enable</i>	Enable NP4 or NP6XLITE offloading (fast path).											
Option	Description																	
<i>disable</i>	Disable NP4 or NP6XLITE offloading (fast path).																	
<i>enable</i>	Enable NP4 or NP6XLITE offloading (fast path).																	
garbage-session-collector	Enable/disable garbage session collector.	option	-	disable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable garbage session collector.</td></tr><tr><td><i>enable</i></td><td>Enable garbage session collector.</td></tr></table>	Option	Description	<i>disable</i>	Disable garbage session collector.	<i>enable</i>	Enable garbage session collector.											
Option	Description																	
<i>disable</i>	Disable garbage session collector.																	
<i>enable</i>	Enable garbage session collector.																	
ipsec-STs-timeout	Set NP6XLite IPsec STS msg timeout.	option	-	5														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>1</td><td>Set NP6Xlite STS message timeout to 1 sec (recommended for IPSec throughput GUI).</td></tr><tr><td>2</td><td>Set NP6Xlite STS message timeout to 2 sec.</td></tr><tr><td>3</td><td>Set NP6Xlite STS message timeout to 3 sec.</td></tr><tr><td>4</td><td>Set NP6Xlite STS message timeout to 4 sec.</td></tr><tr><td>5</td><td>Set NP6Xlite STS message timeout to 5 sec (default).</td></tr><tr><td>6</td><td>Set NP6Xlite STS message timeout to 6 sec.</td></tr></table>	Option	Description	1	Set NP6Xlite STS message timeout to 1 sec (recommended for IPSec throughput GUI).	2	Set NP6Xlite STS message timeout to 2 sec.	3	Set NP6Xlite STS message timeout to 3 sec.	4	Set NP6Xlite STS message timeout to 4 sec.	5	Set NP6Xlite STS message timeout to 5 sec (default).	6	Set NP6Xlite STS message timeout to 6 sec.			
Option	Description																	
1	Set NP6Xlite STS message timeout to 1 sec (recommended for IPSec throughput GUI).																	
2	Set NP6Xlite STS message timeout to 2 sec.																	
3	Set NP6Xlite STS message timeout to 3 sec.																	
4	Set NP6Xlite STS message timeout to 4 sec.																	
5	Set NP6Xlite STS message timeout to 5 sec (default).																	
6	Set NP6Xlite STS message timeout to 6 sec.																	

Parameter	Description	Type	Size	Default																																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>7</td><td>Set NP6Xlite STS message timeout to 7 sec.</td></tr><tr><td>8</td><td>Set NP6Xlite STS message timeout to 8 sec.</td></tr><tr><td>9</td><td>Set NP6Xlite STS message timeout to 9 sec.</td></tr><tr><td>10</td><td>Set NP6Xlite STS message timeout to 10 sec.</td></tr></table>	Option	Description	7	Set NP6Xlite STS message timeout to 7 sec.	8	Set NP6Xlite STS message timeout to 8 sec.	9	Set NP6Xlite STS message timeout to 9 sec.	10	Set NP6Xlite STS message timeout to 10 sec.																									
	Option	Description																																		
	7	Set NP6Xlite STS message timeout to 7 sec.																																		
	8	Set NP6Xlite STS message timeout to 8 sec.																																		
	9	Set NP6Xlite STS message timeout to 9 sec.																																		
10	Set NP6Xlite STS message timeout to 10 sec.																																			
ipsec-inner-fragment	Enable/disable NP6XLite IPsec fragmentation type: inner.	option	-	disable																																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>NP6XLite ipsec fragmentation type: outer.</td></tr><tr><td>enable</td><td>Enable NP6XLite ipsec fragmentation type: inner.</td></tr></table>	Option	Description	disable	NP6XLite ipsec fragmentation type: outer.	enable	Enable NP6XLite ipsec fragmentation type: inner.																													
	Option	Description																																		
	disable	NP6XLite ipsec fragmentation type: outer.																																		
enable	Enable NP6XLite ipsec fragmentation type: inner.																																			
ipsec-throughput-msg-frequency	Set NP6XLite IPsec throughput msg frequency: 0--disable 1--32KB 3--64KB ... 0x3fff--256MB 0x7fff--512MB 0xffff--1GB.	option	-	disable																																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable NP6Xlite throughput update message.</td></tr><tr><td>32KB</td><td>Set NP6Xlite throughput update message frequency to 32KB.</td></tr><tr><td>64KB</td><td>Set NP6Xlite throughput update message frequency to 64KB.</td></tr><tr><td>128KB</td><td>Set NP6Xlite throughput update message frequency to 128KB.</td></tr><tr><td>256KB</td><td>Set NP6Xlite throughput update message frequency to 256KB.</td></tr><tr><td>512KB</td><td>Set NP6Xlite throughput update message frequency to 512KB.</td></tr><tr><td>1MB</td><td>Set NP6Xlite throughput update message frequency to 1MB.</td></tr><tr><td>2MB</td><td>Set NP6Xlite throughput update message frequency to 2MB.</td></tr><tr><td>4MB</td><td>Set NP6Xlite throughput update message frequency to 4MB.</td></tr><tr><td>8MB</td><td>Set NP6Xlite throughput update message frequency to 8MB.</td></tr><tr><td>16MB</td><td>Set NP6Xlite throughput update message frequency to 16MB.</td></tr><tr><td>32MB</td><td>Set NP6Xlite throughput update message frequency to 32MB.</td></tr><tr><td>64MB</td><td>Set NP6Xlite throughput update message frequency to 64MB.</td></tr><tr><td>128MB</td><td>Set NP6Xlite throughput update message frequency to 128MB.</td></tr><tr><td>256MB</td><td>Set NP6Xlite throughput update message frequency to 256MB.</td></tr></table>	Option	Description	disable	Disable NP6Xlite throughput update message.	32KB	Set NP6Xlite throughput update message frequency to 32KB.	64KB	Set NP6Xlite throughput update message frequency to 64KB.	128KB	Set NP6Xlite throughput update message frequency to 128KB.	256KB	Set NP6Xlite throughput update message frequency to 256KB.	512KB	Set NP6Xlite throughput update message frequency to 512KB.	1MB	Set NP6Xlite throughput update message frequency to 1MB.	2MB	Set NP6Xlite throughput update message frequency to 2MB.	4MB	Set NP6Xlite throughput update message frequency to 4MB.	8MB	Set NP6Xlite throughput update message frequency to 8MB.	16MB	Set NP6Xlite throughput update message frequency to 16MB.	32MB	Set NP6Xlite throughput update message frequency to 32MB.	64MB	Set NP6Xlite throughput update message frequency to 64MB.	128MB	Set NP6Xlite throughput update message frequency to 128MB.	256MB	Set NP6Xlite throughput update message frequency to 256MB.			
	Option	Description																																		
	disable	Disable NP6Xlite throughput update message.																																		
	32KB	Set NP6Xlite throughput update message frequency to 32KB.																																		
	64KB	Set NP6Xlite throughput update message frequency to 64KB.																																		
	128KB	Set NP6Xlite throughput update message frequency to 128KB.																																		
	256KB	Set NP6Xlite throughput update message frequency to 256KB.																																		
	512KB	Set NP6Xlite throughput update message frequency to 512KB.																																		
	1MB	Set NP6Xlite throughput update message frequency to 1MB.																																		
	2MB	Set NP6Xlite throughput update message frequency to 2MB.																																		
	4MB	Set NP6Xlite throughput update message frequency to 4MB.																																		
	8MB	Set NP6Xlite throughput update message frequency to 8MB.																																		
	16MB	Set NP6Xlite throughput update message frequency to 16MB.																																		
	32MB	Set NP6Xlite throughput update message frequency to 32MB.																																		
	64MB	Set NP6Xlite throughput update message frequency to 64MB.																																		
128MB	Set NP6Xlite throughput update message frequency to 128MB.																																			
256MB	Set NP6Xlite throughput update message frequency to 256MB.																																			



Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	512MB	Set NP6Xlite throughput update message frequency to 512MB.		
	1GB	Set NP6Xlite throughput update message frequency to 1GB.		
name	Device Name.	string	Maximum length: 31	
per-session-accounting	Enable/disable per-session accounting.	option	-	traffic-log-only
	<b>Option</b>	<b>Description</b>		
	disable	Disable per-session accounting.		
	traffic-log-only	Per-session accounting only for sessions with traffic logging enabled in firewall policy.		
	enable	Per-session accounting for all sessions.		
session-collector-interval	Set garbage session collection cleanup interval.	integer	Minimum value: 1 Maximum value: 100	64
session-timeout-fixed	Enable/disable fixed timeout interval mode.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	disable	Disable NPU session timeout at fixed interval.		
	enable	Enable NPU session timeout at fixed interval.		
session-timeout-interval	Set session timeout interval.	integer	Minimum value: 0 Maximum value: 1000	40
session-timeout-random-range	Set the randomization range.	integer	Minimum value: 0 Maximum value: 1000	8

### config fp-anomaly

Parameter	Description	Type	Size	Default
tcp-syn-fin	TCP SYN flood SYN/FIN flag set anomalies.	option	-	allow

Parameter	Description	Type	Size	Default
	<b>Option</b> <b>Description</b>			
	<i>allow</i>	Allow TCP packets with syn_fin flag set to pass.		
	<i>drop</i>	Drop TCP packets with syn_fin flag set.		
	<i>trap-to-host</i>	Forward TCP packets with syn_fin flag set to FortiOS.		
tcp-fin-noack	TCP SYN flood with FIN flag set without ACK setting anomalies.	option	-	trap-to-host
	<b>Option</b> <b>Description</b>			
	<i>allow</i>	Allow TCP packets with FIN flag set without ack setting to pass.		
	<i>drop</i>	Drop TCP packets with FIN flag set without ack setting.		
	<i>trap-to-host</i>	Forward TCP packets with FIN flag set without ack setting to FortiOS.		
tcp-fin-only	TCP SYN flood with only FIN flag set anomalies.	option	-	trap-to-host
	<b>Option</b> <b>Description</b>			
	<i>allow</i>	Allow TCP packets with FIN flag set only to pass.		
	<i>drop</i>	Drop TCP packets with FIN flag set only.		
	<i>trap-to-host</i>	Forward TCP packets with FIN flag set only to FortiOS.		
tcp-no-flag	TCP SYN flood with no flag set anomalies.	option	-	allow
	<b>Option</b> <b>Description</b>			
	<i>allow</i>	Allow TCP packets without flag set to pass.		
	<i>drop</i>	Drop TCP packets without flag set.		
	<i>trap-to-host</i>	Forward TCP packets without flag set to FortiOS.		
tcp-syn-data	TCP SYN flood packets with data anomalies.	option	-	allow
	<b>Option</b> <b>Description</b>			
	<i>allow</i>	Allow TCP syn packets with data to pass.		
	<i>drop</i>	Drop TCP syn packets with data.		
	<i>trap-to-host</i>	Forward TCP syn packets with data to FortiOS.		
tcp-winnuke	TCP WinNuke anomalies.	option	-	trap-to-host
	<b>Option</b> <b>Description</b>			
	<i>allow</i>	Allow TCP packets winnuke attack to pass.		

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>drop</i>	Drop TCP packets winnuke attack.		
	<i>trap-to-host</i>	Forward TCP packets winnuke attack to FortiOS.		
tcp-land	TCP land anomalies.	option	-	trap-to-host
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow TCP land attack to pass.		
	<i>drop</i>	Drop TCP land attack.		
	<i>trap-to-host</i>	Forward TCP land attack to FortiOS.		
udp-land	UDP land anomalies.	option	-	trap-to-host
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow UDP land attack to pass.		
	<i>drop</i>	Drop UDP land attack.		
	<i>trap-to-host</i>	Forward UDP land attack to FortiOS.		
icmp-land	ICMP land anomalies.	option	-	trap-to-host
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow ICMP land attack to pass.		
	<i>drop</i>	Drop ICMP land attack.		
	<i>trap-to-host</i>	Forward ICMP land attack to FortiOS.		
icmp-frag	Layer 3 fragmented packets that could be part of layer 4 ICMP anomalies.	option	-	allow
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow L3 fragment packet with L4 protocol as ICMP attack to pass.		
	<i>drop</i>	Drop L3 fragment packet with L4 protocol as ICMP attack.		
	<i>trap-to-host</i>	Forward L3 fragment packet with L4 protocol as ICMP attack to FortiOS.		
ipv4-land	Land anomalies.	option	-	trap-to-host
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow IPv4 land attack to pass.		
	<i>drop</i>	Drop IPv4 land attack.		

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>trap-to-host</td><td>Forward IPv4 land attack to FortiOS.</td></tr></table>	Option	Description	trap-to-host	Forward IPv4 land attack to FortiOS.							
	Option	Description										
	trap-to-host	Forward IPv4 land attack to FortiOS.										
ipv4-proto-err	Invalid layer 4 protocol anomalies.	option	-	trap-to-host								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allow IPv4 invalid L4 protocol to pass.</td></tr><tr><td>drop</td><td>Drop IPv4 invalid L4 protocol.</td></tr><tr><td>trap-to-host</td><td>Forward IPv4 invalid L4 protocol to FortiOS.</td></tr></table>	Option	Description	allow	Allow IPv4 invalid L4 protocol to pass.	drop	Drop IPv4 invalid L4 protocol.	trap-to-host	Forward IPv4 invalid L4 protocol to FortiOS.			
	Option	Description										
	allow	Allow IPv4 invalid L4 protocol to pass.										
	drop	Drop IPv4 invalid L4 protocol.										
trap-to-host	Forward IPv4 invalid L4 protocol to FortiOS.											
ipv4-unknopt	Unknown option anomalies.	option	-	trap-to-host								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allow IPv4 with unknown options to pass.</td></tr><tr><td>drop</td><td>Drop IPv4 with unknown options.</td></tr><tr><td>trap-to-host</td><td>Forward IPv4 with unknown options to FortiOS.</td></tr></table>	Option	Description	allow	Allow IPv4 with unknown options to pass.	drop	Drop IPv4 with unknown options.	trap-to-host	Forward IPv4 with unknown options to FortiOS.			
	Option	Description										
	allow	Allow IPv4 with unknown options to pass.										
	drop	Drop IPv4 with unknown options.										
trap-to-host	Forward IPv4 with unknown options to FortiOS.											
ipv4-optrr	Record route option anomalies.	option	-	trap-to-host								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allow IPv4 with record route option to pass.</td></tr><tr><td>drop</td><td>Drop IPv4 with record route option.</td></tr><tr><td>trap-to-host</td><td>Forward IPv4 with record route option to FortiOS.</td></tr></table>	Option	Description	allow	Allow IPv4 with record route option to pass.	drop	Drop IPv4 with record route option.	trap-to-host	Forward IPv4 with record route option to FortiOS.			
	Option	Description										
	allow	Allow IPv4 with record route option to pass.										
	drop	Drop IPv4 with record route option.										
trap-to-host	Forward IPv4 with record route option to FortiOS.											
ipv4-optssrr	Strict source record route option anomalies.	option	-	trap-to-host								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allow IPv4 with strict source record route option to pass.</td></tr><tr><td>drop</td><td>Drop IPv4 with strict source record route option.</td></tr><tr><td>trap-to-host</td><td>Forward IPv4 with strict source record route option to FortiOS.</td></tr></table>	Option	Description	allow	Allow IPv4 with strict source record route option to pass.	drop	Drop IPv4 with strict source record route option.	trap-to-host	Forward IPv4 with strict source record route option to FortiOS.			
	Option	Description										
	allow	Allow IPv4 with strict source record route option to pass.										
	drop	Drop IPv4 with strict source record route option.										
trap-to-host	Forward IPv4 with strict source record route option to FortiOS.											
ipv4-optlsrr	Loose source record route option anomalies.	option	-	trap-to-host								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allow IPv4 with loose source record route option to pass.</td></tr><tr><td>drop</td><td>Drop IPv4 with loose source record route option.</td></tr><tr><td>trap-to-host</td><td>Forward IPv4 with loose source record route option to FortiOS.</td></tr></table>	Option	Description	allow	Allow IPv4 with loose source record route option to pass.	drop	Drop IPv4 with loose source record route option.	trap-to-host	Forward IPv4 with loose source record route option to FortiOS.			
	Option	Description										
	allow	Allow IPv4 with loose source record route option to pass.										
	drop	Drop IPv4 with loose source record route option.										
trap-to-host	Forward IPv4 with loose source record route option to FortiOS.											
ipv4-optstream	Stream option anomalies.	option	-	trap-to-host								

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow IPv4 with stream option to pass.		
	<i>drop</i>	Drop IPv4 with stream option.		
	<i>trap-to-host</i>	Forward IPv4 with stream option to FortiOS.		
ipv4-optsecurity	Security option anomalies.	option	-	trap-to-host
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow IPv4 with security option to pass.		
	<i>drop</i>	Drop IPv4 with security option.		
	<i>trap-to-host</i>	Forward IPv4 with security option to FortiOS.		
ipv4-opttimestamp	Timestamp option anomalies.	option	-	trap-to-host
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow IPv4 with timestamp option to pass.		
	<i>drop</i>	Drop IPv4 with timestamp option.		
	<i>trap-to-host</i>	Forward IPv4 with timestamp option to FortiOS.		
ipv4-csum-err	Invalid IPv4 IP checksum anomalies.	option	-	drop
	<b>Option</b>	<b>Description</b>		
	<i>drop</i>	Drop IPv4 invalid IP checksum.		
	<i>trap-to-host</i>	Forward IPv4 invalid IP checksum to main CPU for processing.		
tcp-csum-err	Invalid IPv4 TCP checksum anomalies.	option	-	drop
	<b>Option</b>	<b>Description</b>		
	<i>drop</i>	Drop IPv4 invalid TCP checksum.		
	<i>trap-to-host</i>	Forward IPv4 invalid TCP checksum to main CPU for processing.		
udp-csum-err	Invalid IPv4 UDP checksum anomalies.	option	-	drop
	<b>Option</b>	<b>Description</b>		
	<i>drop</i>	Drop IPv4 invalid UDP checksum.		
	<i>trap-to-host</i>	Forward IPv4 invalid UDP checksum to main CPU for processing.		
icmp-csum-err	Invalid IPv4 ICMP checksum anomalies.	option	-	drop

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>drop</td><td>Drop IPv4 invalid ICMP checksum.</td></tr><tr><td>trap-to-host</td><td>Forward IPv4 invalid ICMP checksum to main CPU for processing.</td></tr></table>	Option	Description	drop	Drop IPv4 invalid ICMP checksum.	trap-to-host	Forward IPv4 invalid ICMP checksum to main CPU for processing.					
	Option	Description										
	drop	Drop IPv4 invalid ICMP checksum.										
	trap-to-host	Forward IPv4 invalid ICMP checksum to main CPU for processing.										
ipv6-land	Land anomalies.	option	-	trap-to-host								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allow IPv6 land attack to pass.</td></tr><tr><td>drop</td><td>Drop IPv6 land attack.</td></tr><tr><td>trap-to-host</td><td>Forward IPv6 land attack to FortiOS.</td></tr></table>	Option	Description	allow	Allow IPv6 land attack to pass.	drop	Drop IPv6 land attack.	trap-to-host	Forward IPv6 land attack to FortiOS.			
	Option	Description										
	allow	Allow IPv6 land attack to pass.										
	drop	Drop IPv6 land attack.										
trap-to-host	Forward IPv6 land attack to FortiOS.											
ipv6-proto-err	Layer 4 invalid protocol anomalies.	option	-	trap-to-host								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allow IPv6 L4 invalid protocol to pass.</td></tr><tr><td>drop</td><td>Drop IPv6 L4 invalid protocol.</td></tr><tr><td>trap-to-host</td><td>Forward IPv6 L4 invalid protocol to FortiOS.</td></tr></table>	Option	Description	allow	Allow IPv6 L4 invalid protocol to pass.	drop	Drop IPv6 L4 invalid protocol.	trap-to-host	Forward IPv6 L4 invalid protocol to FortiOS.			
	Option	Description										
	allow	Allow IPv6 L4 invalid protocol to pass.										
	drop	Drop IPv6 L4 invalid protocol.										
trap-to-host	Forward IPv6 L4 invalid protocol to FortiOS.											
ipv6-unknpt	Unknown option anomalies.	option	-	trap-to-host								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allow IPv6 with unknown options to pass.</td></tr><tr><td>drop</td><td>Drop IPv6 with unknown options.</td></tr><tr><td>trap-to-host</td><td>Forward IPv6 with unknown options to FortiOS.</td></tr></table>	Option	Description	allow	Allow IPv6 with unknown options to pass.	drop	Drop IPv6 with unknown options.	trap-to-host	Forward IPv6 with unknown options to FortiOS.			
	Option	Description										
	allow	Allow IPv6 with unknown options to pass.										
	drop	Drop IPv6 with unknown options.										
trap-to-host	Forward IPv6 with unknown options to FortiOS.											
ipv6-saddr-err	Source address as multicast anomalies.	option	-	trap-to-host								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allow IPv6 with source address as multicast to pass.</td></tr><tr><td>drop</td><td>Drop IPv6 with source address as multicast.</td></tr><tr><td>trap-to-host</td><td>Forward IPv6 with source address as multicast to FortiOS.</td></tr></table>	Option	Description	allow	Allow IPv6 with source address as multicast to pass.	drop	Drop IPv6 with source address as multicast.	trap-to-host	Forward IPv6 with source address as multicast to FortiOS.			
	Option	Description										
	allow	Allow IPv6 with source address as multicast to pass.										
	drop	Drop IPv6 with source address as multicast.										
trap-to-host	Forward IPv6 with source address as multicast to FortiOS.											
ipv6-daddr-err	Destination address as unspecified or loopback address anomalies.	option	-	trap-to-host								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allow IPv6 with destination address as unspecified or loopback address to pass.</td></tr></table>	Option	Description	allow	Allow IPv6 with destination address as unspecified or loopback address to pass.							
	Option	Description										
allow	Allow IPv6 with destination address as unspecified or loopback address to pass.											

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>drop</i>	Drop IPv6 with destination address as unspecified or loopback address.		
	<i>trap-to-host</i>	Forward IPv6 with destination address as unspecified or loopback address to FortiOS.		
ipv6-optralert	Router alert option anomalies.	option	-	trap-to-host
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow IPv6 with router alert option to pass.		
	<i>drop</i>	Drop IPv6 with router alert option.		
	<i>trap-to-host</i>	Forward IPv6 with router alert option to FortiOS.		
ipv6-optjumbo	Jumbo options anomalies.	option	-	trap-to-host
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow IPv6 with jumbo option to pass.		
	<i>drop</i>	Drop IPv6 with jumbo option.		
	<i>trap-to-host</i>	Forward IPv6 with jumbo option to FortiOS.		
ipv6-opttunnel	Tunnel encapsulation limit option anomalies.	option	-	trap-to-host
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow IPv6 with tunnel encapsulation limit to pass.		
	<i>drop</i>	Drop IPv6 with tunnel encapsulation limit.		
	<i>trap-to-host</i>	Forward IPv6 with tunnel encapsulation limit to FortiOS.		
ipv6-opthomeaddr	Home address option anomalies.	option	-	trap-to-host
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow IPv6 with home address option to pass.		
	<i>drop</i>	Drop IPv6 with home address option.		
	<i>trap-to-host</i>	Forward IPv6 with home address option to FortiOS.		
ipv6-optnsap	Network service access point address option anomalies.	option	-	trap-to-host

Parameter	Description	Type	Size	Default
	Option	Description		
	allow	Allow IPv6 with network service access point address option to pass.		
	drop	Drop IPv6 with network service access point address option.		
	trap-to-host	Forward IPv6 with network service access point address option to FortiOS.		
ipv6-optendpid	End point identification anomalies.	option	-	trap-to-host
	Option	Description		
	allow	Allow IPv6 with end point identification option to pass.		
	drop	Drop IPv6 with end point identification option.		
	trap-to-host	Forward IPv6 with end point identification option to FortiOS.		
ipv6-optinvld	Invalid option anomalies.Invalid option anomalies.	option	-	trap-to-host
	Option	Description		
	allow	Allow IPv6 with invalid option to pass.		
	drop	Drop IPv6 with invalid option.		
	trap-to-host	Forward IPv6 with invalid option to FortiOS.		

## config hpe

Parameter	Description	Type	Size	Default
tcpsyn-max	Maximum TCP SYN packet rate.	integer	Minimum value: 10000 Maximum value: 4000000000	5000000
tcp-max	Maximum TCP packet rate.	integer	Minimum value: 10000 Maximum value: 4000000000	5000000
udp-max	Maximum UDP packet rate.	integer	Minimum value: 10000 Maximum value: 4000000000	5000000



Parameter	Description	Type	Size	Default						
icmp-max	Maximum ICMP packet rate.	integer	Minimum value: 10000 Maximum value: 4000000000	1000000						
sctp-max	Maximum SCTP packet rate.	integer	Minimum value: 10000 Maximum value: 4000000000	1000000						
esp-max	Maximum ESP packet rate.	integer	Minimum value: 10000 Maximum value: 4000000000	1000000						
ip-frag-max	Maximum fragmented IP packet rate.	integer	Minimum value: 10000 Maximum value: 4000000000	1000000						
ip-others-max	Maximum IP packet rate for other packets.	integer	Minimum value: 10000 Maximum value: 4000000000	1000000						
arp-max	Maximum ARP packet rate.	integer	Minimum value: 10000 Maximum value: 4000000000	1000000						
l2-others-max	Maximum L2 packet rate for L2 packets that are not ARP packets.	integer	Minimum value: 10000 Maximum value: 4000000000	1000000						
enable-shaper	Enable/Disable NPU host protection engine (HPE) shaper.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable NPU HPE shaping based on packet type.</td></tr><tr><td>enable</td><td>Enable NPU HPE shaping based on packet type.</td></tr></table>				Option	Description	disable	Disable NPU HPE shaping based on packet type.	enable	Enable NPU HPE shaping based on packet type.
Option	Description									
disable	Disable NPU HPE shaping based on packet type.									
enable	Enable NPU HPE shaping based on packet type.									

## config system npu-setting prp



This command is available for model(s): FortiGate 100F, FortiGate 101F, FortiGate 60F, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 60F, FortiWiFi 61F.

It is not available for: FortiGate 1000D, FortiGate 100EF, FortiGate 100E, FortiGate 101E, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 61E, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate VM64, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 61E, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

Configure NPU PRP attributes.

```
config system npu-setting prp
    Description: Configure NPU PRP attributes.
    set prp-port-in <interface-name1>, <interface-name2>, ...
    set prp-port-out <interface-name1>, <interface-name2>, ...
end
```

## config system npu-setting prp

Parameter	Description	Type	Size	Default
prp-port-in <interface-name>	Ingress port configured to allow the PRP trailer not be stripped off when the PRP packets come in. All of the traffic originating from these ports will always be sent to the host. Physical interface name.	string	Maximum length: 35	
prp-port-out <interface-name>	Egress port configured to allow the PRP trailer not be stripped off when the PRP packets go out. Physical interface name.	string	Maximum length: 35	

## config system npu-vlink



This command is available for model(s): FortiGate 1800F, FortiGate 1801F, FortiGate 2600F, FortiGate 2601F, FortiGate 3000F, FortiGate 3001F, FortiGate 3500F, FortiGate 3501F, FortiGate 400F, FortiGate 401F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 600F, FortiGate 601F.

It is not available for: FortiGate 1000D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 3000D, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 401E, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 601E, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

Configure NPU VDOM link.

```
config system npu-vlink
    Description: Configure NPU VDOM link.
    edit <name>
    next
end
```

## config system npu-vlink

Parameter	Description	Type	Size	Default
name	NPU VDOM link name (maximum = 14 characters).	string	Maximum length: 19	

## config system npu



This command is available for model(s): FortiGate 1000D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 90E, FortiGate 91E, FortiGate VM64.

### Configure NPU attributes.

```
config system npu
  Description: Configure NPU attributes.
  config background-sse-scan
    Description: Configure driver background scan for SSE.
    set scan [disable|enable]
    set stats-update-interval {integer}
    set udp-keepalive-interval {integer}
  end
  set capwap-offload [enable|disable]
  set dedicated-management-affinity {string}
  set dedicated-management-cpu [enable|disable]
  set default-qos-type [policing|shaping]
  config dos-options
    Description: NPU DoS configurations.
    set npu-dos-meter-mode [global|local]
    set npu-dos-tpe-mode [enable|disable]
  end
  set double-level-mcast-offload [enable|disable]
  set dse-timeout {integer}
  config dsw-dts-profile
    Description: Configure NPU DSW DTS profile.
    edit <profile-id>
      set min-limit {integer}
      set step {integer}
      set action [wait|drop|...]
    end
  next
```

```

end
config dsw-queue-dts-profile
    Description: Configure NPU DSW Queue DTS profile.
    edit <name>
        set iport [EIF0|EIF1|...]
        set oport [EIF0|EIF1|...]
        set profile-id {integer}
        set queue-select {integer}
    next
end
set fastpath [disable|enable]
config fp-anomaly
    Description: NP6Lite anomaly protection (packet drop or send trap to host).
    set ipv4-ver-err [drop|trap-to-host]
    set ipv4-ihl-err [drop|trap-to-host]
    set ipv4-len-err [drop|trap-to-host]
    set ipv4-ttlzero-err [drop|trap-to-host]
    set ipv4-csum-err [drop|trap-to-host]
    set ipv4-opt-err [drop|trap-to-host]
    set tcp-hlen-err [drop|trap-to-host]
    set tcp-plen-err [drop|trap-to-host]
    set tcp-csum-err [drop|trap-to-host]
    set udp-plen-err [drop|trap-to-host]
    set udp-hlen-err [drop|trap-to-host]
    set udp-csum-err [drop|trap-to-host]
    set udp-len-err [drop|trap-to-host]
    set udplite-cover-err [drop|trap-to-host]
    set udplite-csum-err [drop|trap-to-host]
    set icmp-minlen-err [drop|trap-to-host]
    set icmp-csum-err [drop|trap-to-host]
    set esp-minlen-err [drop|trap-to-host]
    set unknproto-minlen-err [drop|trap-to-host]
    set ipv6-ver-err [drop|trap-to-host]
    set ipv6-ihl-err [drop|trap-to-host]
    set ipv6-plen-zero [drop|trap-to-host]
    set ipv6-exthdr-order-err [drop|trap-to-host]
    set ipv6-exthdr-len-err [drop|trap-to-host]
end
set gtp-enhanced-cpu-range [0|1|...]
set gtp-enhanced-mode [enable|disable]
set gtp-support [enable|disable]
set hash-tbl-spread [enable|disable]
set host-shortcut-mode [bi-directional|host-shortcut]
config hpe
    Description: Host protection engine configuration.
    set all-protocol {integer}
    set tcpsyn-max {integer}
    set tcpsyn-ack-max {integer}
    set tcpfin-rst-max {integer}
    set tcp-max {integer}
    set udp-max {integer}
    set icmp-max {integer}
    set sctp-max {integer}
    set esp-max {integer}
    set ip-frag-max {integer}
    set ip-others-max {integer}

```

```

        set arp-max {integer}
        set l2-others-max {integer}
        set high-priority {integer}
        set enable-shaper [disable|enable]
    end
    set htab-dedi-queue-nr {integer}
    set htab-msg-queue [data|idle|...]
    set htx-gtse-quota [100Mbps|200Mbps|...]
    set htx-icmp-csum-chk [drop|pass]
    set hw-ha-scan-interval {integer}
    set inbound-dscp-copy-port <interface1>, <interface2>, ...
    set intf-shaping-offload [enable|disable]
    set ip-fragment-offload [disable|enable]
    config ip-reassembly
        Description: IP reassembly engine configuration.
        set min-timeout {integer}
        set max-timeout {integer}
        set status [disable|enable]
    end
    set iph-rsvd-re-cksum [enable|disable]
    set ippool-overload-high {integer}
    set ippool-overload-low {integer}
    set ipsec-dec-subengine-mask {user}
    set ipsec-enc-subengine-mask {user}
    set ipsec-inbound-cache [enable|disable]
    set ipsec-mtu-override [disable|enable]
    set ipsec-ob-np-sel [rr|Packet|...]
    set ipsec-over-vlink [enable|disable]
    config isf-np-queues
        Description: Configure queues of switch port connected to NP6 XAUI on ingress path.
        set cos0 {string}
        set cos1 {string}
        set cos2 {string}
        set cos3 {string}
        set cos4 {string}
        set cos5 {string}
        set cos6 {string}
        set cos7 {string}
    end
    set lag-out-port-select [disable|enable]
    set max-session-timeout {integer}
    set mcast-session-accounting [tpe-based|session-based|...]
    set napi-break-interval {integer}
    set nat46-force-ipv4-packet-forwarding [enable|disable]
    config np-queues
        Description: Configure queue assignment on NP7.
        config profile
            Description: Configure a NP7 class profile.
            edit <id>
                set type [cos|dscp]
                set weight {integer}
                set cos0 [queue0|queue1|...]
                set cos1 [queue0|queue1|...]
                set cos2 [queue0|queue1|...]
                set cos3 [queue0|queue1|...]
                set cos4 [queue0|queue1|...]
            end
        end
    end

```

---

```
set cos5 [queue0|queue1|...]
set cos6 [queue0|queue1|...]
set cos7 [queue0|queue1|...]
set dscp0 [queue0|queue1|...]
set dscp1 [queue0|queue1|...]
set dscp2 [queue0|queue1|...]
set dscp3 [queue0|queue1|...]
set dscp4 [queue0|queue1|...]
set dscp5 [queue0|queue1|...]
set dscp6 [queue0|queue1|...]
set dscp7 [queue0|queue1|...]
set dscp8 [queue0|queue1|...]
set dscp9 [queue0|queue1|...]
set dscp10 [queue0|queue1|...]
set dscp11 [queue0|queue1|...]
set dscp12 [queue0|queue1|...]
set dscp13 [queue0|queue1|...]
set dscp14 [queue0|queue1|...]
set dscp15 [queue0|queue1|...]
set dscp16 [queue0|queue1|...]
set dscp17 [queue0|queue1|...]
set dscp18 [queue0|queue1|...]
set dscp19 [queue0|queue1|...]
set dscp20 [queue0|queue1|...]
set dscp21 [queue0|queue1|...]
set dscp22 [queue0|queue1|...]
set dscp23 [queue0|queue1|...]
set dscp24 [queue0|queue1|...]
set dscp25 [queue0|queue1|...]
set dscp26 [queue0|queue1|...]
set dscp27 [queue0|queue1|...]
set dscp28 [queue0|queue1|...]
set dscp29 [queue0|queue1|...]
set dscp30 [queue0|queue1|...]
set dscp31 [queue0|queue1|...]
set dscp32 [queue0|queue1|...]
set dscp33 [queue0|queue1|...]
set dscp34 [queue0|queue1|...]
set dscp35 [queue0|queue1|...]
set dscp36 [queue0|queue1|...]
set dscp37 [queue0|queue1|...]
set dscp38 [queue0|queue1|...]
set dscp39 [queue0|queue1|...]
set dscp40 [queue0|queue1|...]
set dscp41 [queue0|queue1|...]
set dscp42 [queue0|queue1|...]
set dscp43 [queue0|queue1|...]
set dscp44 [queue0|queue1|...]
set dscp45 [queue0|queue1|...]
set dscp46 [queue0|queue1|...]
set dscp47 [queue0|queue1|...]
set dscp48 [queue0|queue1|...]
set dscp49 [queue0|queue1|...]
set dscp50 [queue0|queue1|...]
set dscp51 [queue0|queue1|...]
set dscp52 [queue0|queue1|...]
```

```

        set dscp53 [queue0|queue1|...]
        set dscp54 [queue0|queue1|...]
        set dscp55 [queue0|queue1|...]
        set dscp56 [queue0|queue1|...]
        set dscp57 [queue0|queue1|...]
        set dscp58 [queue0|queue1|...]
        set dscp59 [queue0|queue1|...]
        set dscp60 [queue0|queue1|...]
        set dscp61 [queue0|queue1|...]
        set dscp62 [queue0|queue1|...]
        set dscp63 [queue0|queue1|...]
    next
end
config ethernet-type
    Description: Configure a NP7 QoS Ethernet Type.
    edit <name>
        set type {ether-type}
        set queue {integer}
        set weight {integer}
    next
end
config ip-protocol
    Description: Configure a NP7 QoS IP Protocol.
    edit <name>
        set protocol {integer}
        set queue {integer}
        set weight {integer}
    next
end
config ip-service
    Description: Configure a NP7 QoS IP Service.
    edit <name>
        set protocol {integer}
        set sport {integer}
        set dport {integer}
        set queue {integer}
        set weight {integer}
    next
end
config scheduler
    Description: Configure a NP7 QoS Scheduler.
    edit <name>
        set mode [none|priority|...]
    next
end
end
set np6-cps-optimization-mode [enable|disable]
set pba-eim [disallow|allow]
set per-policy-accounting [disable|enable]
set per-session-accounting [disable|traffic-log-only|...]
set ple-non-syn-tcp-action [forward|drop]
set policy-offload-level [disable|dos-offload]
config port-cpu-map
    Description: Configure NPU interface to CPU core mapping.
    edit <interface>
        set cpu-core {string}

```



```

        next
    end
    config port-npu-map
        Description: Configure port to NPU group mapping.
        edit <interface>
            set npu-group-index {integer}
        next
    end
    config port-path-option
        Description: Configure port using NPU or Intel-NIC.
        set ports-using-npu <interface-name1>, <interface-name2>, ...
    end
    config priority-protocol
        Description: Configure NPU priority protocol.
        set bgp [enable|disable]
        set slbc [enable|disable]
        set bfd [enable|disable]
    end
    set qos-mode [disable|priority|...]
    set qtm-buf-mode [6ch|4ch]
    set rdp-offload [enable|disable]
    set recover-np6-link [enable|disable]
    set session-acct-interval {integer}
    set session-denied-offload [disable|enable]
    set sse-backpressure [enable|disable]
    config sse-ha-scan
        Description: Configure driver HA scan for SSE.
        set gap {integer}
    end
    set strip-clear-text-padding [enable|disable]
    set strip-esp-padding [enable|disable]
    config sw-eh-hash
        Description: Configure switch enhanced hashing.
        set computation [xor16|xor8|...]
        set ip-protocol [include|exclude]
        set source-ip-upper-16 [include|exclude]
        set source-ip-lower-16 [include|exclude]
        set destination-ip-upper-16 [include|exclude]
        set destination-ip-lower-16 [include|exclude]
        set source-port [include|exclude]
        set destination-port [include|exclude]
        set netmask-length {integer}
    end
    set sw-np-bandwidth [0G|2G|...]
    set switch-np-hash [src-ip|dst-ip|...]
    set tcp-rst-timeout {integer}
    config tcp-timeout-profile
        Description: Configure TCP timeout profile.
        edit <id>
            set tcp-idle {integer}
            set fin-wait {integer}
            set close-wait {integer}
            set time-wait {integer}
            set syn-sent {integer}
            set syn-wait {integer}
        next

```

```

end
config udp-timeout-profile
    Description: Configure UDP timeout profile.
    edit <id>
        set udp-idle {integer}
    next
end
set uesp-offload [enable|disable]
set ull-port-mode [10G|25G]
set vlan-lookup-cache [enable|disable]
end

```

## config system npu

Parameter	Description	Type	Size	Default						
capwap-offload *	Enable/disable offloading managed FortiAP and FortiLink CAPWAP sessions.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable CAPWAP offload.</td></tr><tr><td>disable</td><td>Disable CAPWAP offload.</td></tr></table>	Option	Description	enable	Enable CAPWAP offload.	disable	Disable CAPWAP offload.			
Option	Description									
enable	Enable CAPWAP offload.									
disable	Disable CAPWAP offload.									
dedicated-management-affinity *	Affinity setting for management deamons (hexadecimal value up to 256 bits in the format of xxxxxxxxxxxxxxxxx).	string	Maximum length: 79	1						
dedicated-management-cpu *	Enable to dedicate one CPU for GUI and CLI connections when NPs are busy.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable dedication of CPU #0 for management tasks.</td></tr><tr><td>disable</td><td>Disable dedication of CPU #0 for management tasks.</td></tr></table>	Option	Description	enable	Enable dedication of CPU #0 for management tasks.	disable	Disable dedication of CPU #0 for management tasks.			
Option	Description									
enable	Enable dedication of CPU #0 for management tasks.									
disable	Disable dedication of CPU #0 for management tasks.									
default-qos-type *	Set default QoS type.	option	-	shaping						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>policing</td><td>QoS type policing.</td></tr><tr><td>shaping</td><td>QoS type shaping.</td></tr></table>	Option	Description	policing	QoS type policing.	shaping	QoS type shaping.			
Option	Description									
policing	QoS type policing.									
shaping	QoS type shaping.									
double-level-mcast-offload *	Enable double level mcast offload.	option	-	disable						

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable double level mcast offload.</td></tr><tr><td><i>disable</i></td><td>Disable double level mcast offload.</td></tr></table>	Option	Description	<i>enable</i>	Enable double level mcast offload.	<i>disable</i>	Disable double level mcast offload.					
	Option	Description										
	<i>enable</i>	Enable double level mcast offload.										
<i>disable</i>	Disable double level mcast offload.											
dse-timeout *	DSE timeout in seconds.	integer	Minimum value: 0 Maximum value: 3600	10								
fastpath *	Enable/disable NP6 offloading (also called fast path).	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable NP6 offloading (fast path).</td></tr><tr><td><i>enable</i></td><td>Enable NP6 offloading (fast path).</td></tr></table>	Option	Description	<i>disable</i>	Disable NP6 offloading (fast path).	<i>enable</i>	Enable NP6 offloading (fast path).					
	Option	Description										
	<i>disable</i>	Disable NP6 offloading (fast path).										
<i>enable</i>	Enable NP6 offloading (fast path).											
gtp-enhanced-cpu-range *	GTP enhanced CPU range option.	option	-	0								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>0</td><td>Inspect GTPU packets by all CPUs.</td></tr><tr><td>1</td><td>Inspect GTPU packets by Master CPUs.</td></tr><tr><td>2</td><td>Inspect GTPU packets by Slave CPUs.</td></tr></table>	Option	Description	0	Inspect GTPU packets by all CPUs.	1	Inspect GTPU packets by Master CPUs.	2	Inspect GTPU packets by Slave CPUs.			
	Option	Description										
	0	Inspect GTPU packets by all CPUs.										
	1	Inspect GTPU packets by Master CPUs.										
2	Inspect GTPU packets by Slave CPUs.											
gtp-enhanced-mode *	Enable/disable GTP enhanced mode.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable GTP enhanced mode.</td></tr><tr><td><i>disable</i></td><td>Disable GTP enhanced mode.</td></tr></table>	Option	Description	<i>enable</i>	Enable GTP enhanced mode.	<i>disable</i>	Disable GTP enhanced mode.					
	Option	Description										
	<i>enable</i>	Enable GTP enhanced mode.										
<i>disable</i>	Disable GTP enhanced mode.											
gtp-support *	Enable/Disable NP7 GTP support	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable NP7 GTP support</td></tr><tr><td><i>disable</i></td><td>Disable NP7 GTP support</td></tr></table>	Option	Description	<i>enable</i>	Enable NP7 GTP support	<i>disable</i>	Disable NP7 GTP support					
	Option	Description										
	<i>enable</i>	Enable NP7 GTP support										
<i>disable</i>	Disable NP7 GTP support											
hash-tbl-spread *	Enable/disable hash table entry spread.	option	-	enable								

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable hash table entry spread.		
	<i>disable</i>	Disable hash table entry spread.		
host-shortcut-mode *	Set NP6 host shortcut mode.	option	-	bi-directional
	<b>Option</b>	<b>Description</b>		
	<i>bi-directional</i>	Offload TCP and IP Tunnel sessions in both directions between 10G and 1G interfaces (normal operation).		
	<i>host-shortcut</i>	Only offload TCP and IP Tunnel sessions received by 1G interfaces. Select if packets are dropped for offloaded traffic between 10G to 1G interfaces.		
htab-dedi-queue-nr *	Set the number of dedicate queue for hash table messages.	integer	Minimum value: 1 Maximum value: 2	1
htab-msg-queue *	Set hash table message queue mode.	option	-	data
	<b>Option</b>	<b>Description</b>		
	<i>data</i>	Use data queue.		
	<i>idle</i>	Use idle queue.		
	<i>dedicated</i>	Use dedicated queue.		
htx-gtse-quota *	Configure HTX GTSE quota.	option	-	1Gbps
	<b>Option</b>	<b>Description</b>		
	<i>100Mbps</i>	100Mbps.		
	<i>200Mbps</i>	200Mbps.		
	<i>300Mbps</i>	300Mbps.		
	<i>400Mbps</i>	400Mbps.		
	<i>500Mbps</i>	500Mbps.		
	<i>600Mbps</i>	600Mbps.		
	<i>700Mbps</i>	700Mbps.		
	<i>800Mbps</i>	800Mbps.		
	<i>900Mbps</i>	900Mbps.		

Parameter	Description	Type	Size	Default
	<div><div>Option</div><div>Description</div></div>			
	1Gbps1Gbps.			
	2Gbps2Gbps.			
	4Gbps4Gbps.			
	8Gbps8Gbps.			
	10Gbps10Gbps.			
htx-icmp-csum-chk *	Set HTX icmp csum checking mode.	option	-	drop
	<div><div>Option</div><div>Description</div></div>			
	dropDrop bad icmp csum.			
	passPass bad icmp csum.			
hw-ha-scan-interval *	HW HA periodical scan interval in seconds.	integer	Minimum value: 0 Maximum value: 3600	0
inbound-dscp-copy-port <interface> *	Physical interfaces that support inbound-dscp-copy. Physical interface name.	string	Maximum length: 15	
intf-shaping-offload *	Enable/disable NPU offload when doing interface-based traffic shaping according to the egress-shaping-profile.	option	-	disable
	<div><div>Option</div><div>Description</div></div>			
	enableEnable NPU offload when doing interface-based traffic shaping according to the egress-shaping-profile.			
	disableDisable NPU offload when doing interface-based traffic shaping according to the egress-shaping-profile.			
ip-fragment-offload *	Enable/disable NP7 NPU IP fragment offload.	option	-	enable
	<div><div>Option</div><div>Description</div></div>			
	disableDisable IP fragment offload.			
	enableEnable IP fragment offload.			
iph-rsvd-re-csum *	Enable/disable IP checksum re-calculation for packets with iph.reserved bit set.	option	-	disable

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable IP checksum re-calculation for packets with iph.reserved bit set.		
	<i>disable</i>	Disable IP checksum re-calculation for packets with iph.reserved bit set.		
ippool-overload-high *	High threshold for overload ippool port reuse.	integer	Minimum value: 100 Maximum value: 2000	200
ippool-overload-low *	Low threshold for overload ippool port reuse.	integer	Minimum value: 100 Maximum value: 2000	150
ipsec-dec-subengine-mask *	IPsec decryption subengine mask.	user	Not Specified	
ipsec-enc-subengine-mask *	IPsec encryption subengine mask.	user	Not Specified	
ipsec-inbound-cache *	Enable/disable IPsec inbound cache for anti-replay.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable inbound cache always.		
	<i>disable</i>	Disable inbound cache when IPsec anti-replay is on.		
ipsec-mtu-override *	Enable/disable NP6 IPsec MTU override.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable NP6 IPsec MTU override.		
	<i>enable</i>	Enable NP6 IPsec MTU override.		
ipsec-ob-np-sel *	IPsec NP selection for OB SA offloading.	option	-	rr
	<b>Option</b>	<b>Description</b>		
	<i>rr</i>	Round Robin.		
	<i>Packet</i>	NPU of the first packet.		
	<i>Hash</i>	Hash.		
ipsec-over-vlink *	Enable/disable IPsec over vlink.	option	-	disable

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable IPSEC over vlink.</td></tr><tr><td><i>disable</i></td><td>Disable IPSEC over vlink.</td></tr></table>	Option	Description	<i>enable</i>	Enable IPSEC over vlink.	<i>disable</i>	Disable IPSEC over vlink.					
	Option	Description										
	<i>enable</i>	Enable IPSEC over vlink.										
<i>disable</i>	Disable IPSEC over vlink.											
lag-out-port-select *	Enable/disable LAG outgoing port selection based on incoming traffic port.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable LAG outgoing trunk in switch.</td></tr><tr><td><i>enable</i></td><td>Enable LAG outgoing trunk in switch.</td></tr></table>	Option	Description	<i>disable</i>	Disable LAG outgoing trunk in switch.	<i>enable</i>	Enable LAG outgoing trunk in switch.					
	Option	Description										
	<i>disable</i>	Disable LAG outgoing trunk in switch.										
<i>enable</i>	Enable LAG outgoing trunk in switch.											
max-session-timeout *	Maximum time interval for refreshing NPU-offloaded sessions.	integer	Minimum value: 10 Maximum value: 1000	40								
mcast-session-accounting *	Enable/disable traffic accounting for each multicast session through TAE counter.	option	-	tpe-based								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>tpe-based</i></td><td>Enable TPE-based multicast session accounting.</td></tr><tr><td><i>session-based</i></td><td>Enable session-based multicast session accounting.</td></tr><tr><td><i>disable</i></td><td>Disable multicast session accounting.</td></tr></table>	Option	Description	<i>tpe-based</i>	Enable TPE-based multicast session accounting.	<i>session-based</i>	Enable session-based multicast session accounting.	<i>disable</i>	Disable multicast session accounting.			
	Option	Description										
	<i>tpe-based</i>	Enable TPE-based multicast session accounting.										
	<i>session-based</i>	Enable session-based multicast session accounting.										
<i>disable</i>	Disable multicast session accounting.											
napi-break-interval *	NAPI break interval.	integer	Minimum value: 0 Maximum value: 65535	0								
nat46-force-ipv4-packet-forwarding *	Enable/disable mandatory IPv4 packet forwarding in nat46.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable mandatory IPv4 packet forwarding when IPv4 DF is set to 1.</td></tr><tr><td><i>disable</i></td><td>Disable mandatory IPv4 packet forwarding when IPv4 DF is set to 1.</td></tr></table>	Option	Description	<i>enable</i>	Enable mandatory IPv4 packet forwarding when IPv4 DF is set to 1.	<i>disable</i>	Disable mandatory IPv4 packet forwarding when IPv4 DF is set to 1.					
	Option	Description										
	<i>enable</i>	Enable mandatory IPv4 packet forwarding when IPv4 DF is set to 1.										
<i>disable</i>	Disable mandatory IPv4 packet forwarding when IPv4 DF is set to 1.											
np6-cps-optimization-mode *	Enable/disable NP6 connection per second (CPS) optimization mode.	option	-	disable								

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable NP6 connection per second (CPS) optimization mode.		
	<i>disable</i>	Disable NP6 connection per second (CPS) optimization mode.		
pba-eim *	Configure option for PBA(non-overload)/EIM combination.	option	-	allow
	<b>Option</b>	<b>Description</b>		
	<i>disallow</i>	Disallow PBA(non-overload)/EIM combination in SNAT policy.		
	<i>allow</i>	Allow PBA(non-overload)/EIM combination in SNAT policy.		
per-policy-accounting *	Set per-policy accounting.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable per-policy hit count.		
	<i>enable</i>	Enable per-policy hit count		
per-session-accounting *	Enable/disable per-session accounting.	option	-	traffic-log-only
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable per-session accounting.		
	<i>traffic-log-only</i>	Per-session accounting only for sessions with traffic logging enabled in firewall policy.		
	<i>enable</i>	Per-session accounting for all sessions.		
ple-non-syn-tcp-action *	Configure action for the PLE to take on TCP packets that have the SYN field unset.	option	-	forward
	<b>Option</b>	<b>Description</b>		
	<i>forward</i>	PLE forwards all TCP packets to the CPU that have the SYN field unset (default).		
	<i>drop</i>	PLE drops all TCP packets that have the SYN field unset.		
policy-offload-level *	Configure firewall policy offload level.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable policy offloading		



Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>dos-offload</i>	Only enable DoS policy offloading		
qos-mode *	QoS mode on switch and NP.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable QoS on switch and NP.		
	<i>priority</i>	Priority based.		
	<i>round-robin</i>	Round robin scheduler.		
qtm-buf-mode *	QTM channel configuration for packet buffer.	option	-	6ch
	<b>Option</b>	<b>Description</b>		
	<i>6ch</i>	6 DRAM channels for packet buffer.		
	<i>4ch</i>	4 DRAM channels for packet buffer.		
rdp-offload *	Enable/disable RDP offload.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable reliable datagram protocol traffic offload.		
	<i>disable</i>	Disable reliable datagram protocol traffic offload.		
recover-np6-link *	Enable/disable internal link failure check and recovery after boot up.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable internal link failure check and recovery after boot up.		
	<i>disable</i>	Disable internal link failure check and recovery after boot up.		
session-acct-interval *	Session accounting update interval.	integer	Minimum value: 1 Maximum value: 10	5
session-denied-offload *	Enable/disable offloading of denied sessions. Requires ses-denied-traffic to be set.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable offloading of denied sessions.		
	<i>enable</i>	Enable offloading of denied sessions.		

Parameter	Description	Type	Size	Default												
sse-backpressure *	Enable/disable SSE backpressure.	option	-	disable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable SSE backpressure.</td></tr><tr><td><i>disable</i></td><td>Disable SSE backpressure.</td></tr></table>	Option	Description	<i>enable</i>	Enable SSE backpressure.	<i>disable</i>	Disable SSE backpressure.									
Option	Description															
<i>enable</i>	Enable SSE backpressure.															
<i>disable</i>	Disable SSE backpressure.															
strip-clear-text-padding *	Enable/disable stripping clear text padding.	option	-	disable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable stripping clear text padding.</td></tr><tr><td><i>disable</i></td><td>Disable stripping clear text padding.</td></tr></table>	Option	Description	<i>enable</i>	Enable stripping clear text padding.	<i>disable</i>	Disable stripping clear text padding.									
Option	Description															
<i>enable</i>	Enable stripping clear text padding.															
<i>disable</i>	Disable stripping clear text padding.															
strip-esp-padding *	Enable/disable stripping ESP padding.	option	-	disable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable stripping ESP padding.</td></tr><tr><td><i>disable</i></td><td>Disable stripping ESP padding.</td></tr></table>	Option	Description	<i>enable</i>	Enable stripping ESP padding.	<i>disable</i>	Disable stripping ESP padding.									
Option	Description															
<i>enable</i>	Enable stripping ESP padding.															
<i>disable</i>	Disable stripping ESP padding.															
sw-np-bandwidth *	Bandwidth from switch to NP.	option	-	0G												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>0G</i></td><td>Default value. No bandwidth control.</td></tr><tr><td><i>2G</i></td><td>2Gbps.</td></tr><tr><td><i>4G</i></td><td>4Gbps.</td></tr><tr><td><i>5G</i></td><td>5Gbps.</td></tr><tr><td><i>6G</i></td><td>6Gbps.</td></tr></table>	Option	Description	<i>0G</i>	Default value. No bandwidth control.	<i>2G</i>	2Gbps.	<i>4G</i>	4Gbps.	<i>5G</i>	5Gbps.	<i>6G</i>	6Gbps.			
Option	Description															
<i>0G</i>	Default value. No bandwidth control.															
<i>2G</i>	2Gbps.															
<i>4G</i>	4Gbps.															
<i>5G</i>	5Gbps.															
<i>6G</i>	6Gbps.															
switch-np-hash *	Switch-NP trunk port selection Criteria.	option	-	src-dst-ip												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>src-ip</i></td><td>Source IP address.</td></tr><tr><td><i>dst-ip</i></td><td>Destination IP address.</td></tr><tr><td><i>src-dst-ip</i></td><td>Source+dest IP address.</td></tr></table>	Option	Description	<i>src-ip</i>	Source IP address.	<i>dst-ip</i>	Destination IP address.	<i>src-dst-ip</i>	Source+dest IP address.							
Option	Description															
<i>src-ip</i>	Source IP address.															
<i>dst-ip</i>	Destination IP address.															
<i>src-dst-ip</i>	Source+dest IP address.															

Parameter	Description	Type	Size	Default						
tcp-rst-timeout *	TCP RST timeout in seconds.	integer	Minimum value: 0 Maximum value: 16777215	5						
uesp-offload *	Enable/disable UDP-encapsulated ESP offload.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable UDP-encapsulated ESP traffic offload.</td></tr><tr><td>disable</td><td>Disable UDP-encapsulated ESP traffic offload.</td></tr></table>	Option	Description	enable	Enable UDP-encapsulated ESP traffic offload.	disable	Disable UDP-encapsulated ESP traffic offload.			
Option	Description									
enable	Enable UDP-encapsulated ESP traffic offload.									
disable	Disable UDP-encapsulated ESP traffic offload.									
ull-port-mode *	Set ULL port's speed to 10G/25G.	option	-	10G						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>10G</td><td>10G speed setting for ULL ports.</td></tr><tr><td>25G</td><td>25G speed setting for ULL ports.</td></tr></table>	Option	Description	10G	10G speed setting for ULL ports.	25G	25G speed setting for ULL ports.			
Option	Description									
10G	10G speed setting for ULL ports.									
25G	25G speed setting for ULL ports.									
vlan-lookup-cache *	Enable/disable vlan lookup cache.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable VLAN lookup cache.</td></tr><tr><td>disable</td><td>Disable VLAN lookup cache.</td></tr></table>	Option	Description	enable	Enable VLAN lookup cache.	disable	Disable VLAN lookup cache.			
Option	Description									
enable	Enable VLAN lookup cache.									
disable	Disable VLAN lookup cache.									

\* This parameter may not exist in some models.

### config background-sse-scan

Parameter	Description	Type	Size	Default						
scan	Enable/disable background SSE scan by driver thread.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable background sse scan.</td></tr><tr><td><i>enable</i></td><td>Enable background sse scan(default).</td></tr></table>	Option	Description	<i>disable</i>	Disable background sse scan.	<i>enable</i>	Enable background sse scan(default).			
Option	Description									
<i>disable</i>	Disable background sse scan.									
<i>enable</i>	Enable background sse scan(default).									
stats-update-interval	Stats update interval.	integer	Minimum value: 300 Maximum value: 1073741823	300						

Parameter	Description	Type	Size	Default
udp-keepalive-interval	UDP keepalive interval.	integer	Minimum value: 90 Maximum value: 1073741823	90

### config dos-options

Parameter	Description	Type	Size	Default						
npu-dos-meter-mode	Set DoS meter NPU offloading mode.	option	-	global						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>global</i></td><td>Install DoS meter to all NPs.</td></tr><tr><td><i>local</i></td><td>Install DoS meter only to the NP assigned to the traffic.</td></tr></table>				Option	Description	<i>global</i>	Install DoS meter to all NPs.	<i>local</i>	Install DoS meter only to the NP assigned to the traffic.
Option	Description									
<i>global</i>	Install DoS meter to all NPs.									
<i>local</i>	Install DoS meter only to the NP assigned to the traffic.									
npu-dos-tpe-mode	Enable/disable insertion of DoS meter ID to session table.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable insertion of DoS meter ID to session table.</td></tr><tr><td><i>disable</i></td><td>Disable insertion of DoS meter ID to session table.</td></tr></table>				Option	Description	<i>enable</i>	Enable insertion of DoS meter ID to session table.	<i>disable</i>	Disable insertion of DoS meter ID to session table.
Option	Description									
<i>enable</i>	Enable insertion of DoS meter ID to session table.									
<i>disable</i>	Disable insertion of DoS meter ID to session table.									

### config dsw-dts-profile

Parameter	Description	Type	Size	Default
profile-id	Set NPU DSW DTS profile profile id.	integer	Minimum value: 1 Maximum value: 32	0
min-limit	Set NPU DSW DTS profile min-limit.	integer	Minimum value: 32 Maximum value: 2048	0
step	Set NPU DSW DTS profile step.	integer	Minimum value: 0 Maximum value: 64	0
action	Set NPU DSW DTS profile action.	option	-	wait

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>wait</i>	DSW DTS profile WAIT indefinitely.		
	<i>drop</i>	DSW DTS profile DROP immediately.		
	<i>drop_tmr_0</i>	DSW DTS profile DROP after interval #0 time-out.		
	<i>drop_tmr_1</i>	DSW DTS profile DROP after interval #1 time-out.		
	<i>enqueue</i>	DSW DTS profile ENQUEUE immediately.		
	<i>enqueue_0</i>	DSW DTS profile ENQUEUE after interval #0 time-out.		
	<i>enqueue_1</i>	DSW DTS profile ENQUEUE after interval #1 time-out.		

### config dsw-queue-dts-profile

Parameter	Description	Type	Size	Default
name	Name.	string	Maximum length: 35	
iport	Set NPU DSW DTS in port.	option	-	EIF0
	<b>Option</b>	<b>Description</b>		
	<i>EIF0</i>	DSW IPORT EIF0.		
	<i>EIF1</i>	DSW IPORT EIF1.		
	<i>EIF2</i>	DSW IPORT EIF2.		
	<i>EIF3</i>	DSW IPORT EIF3.		
	<i>EIF4</i>	DSW IPORT EIF4.		
	<i>EIF5</i>	DSW IPORT EIF5.		
	<i>EIF6</i>	DSW IPORT EIF6.		
	<i>EIF7</i>	DSW IPORT EIF7.		
	<i>HTX0</i>	DSW IPORT HTX0.		
	<i>HTX1</i>	DSW IPORT HTX1.		
	<i>SSE0</i>	DSW IPORT SSE0.		
	<i>SSE1</i>	DSW IPORT SSE1.		
	<i>SSE2</i>	DSW IPORT SSE2.		
	<i>SSE3</i>	DSW IPORT SSE3.		
	<i>RLT</i>	DSW IPORT RLT.		

Parameter	Description	Type	Size	Default																																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>DFR</i></td><td>DSW IPORT DFR.</td></tr><tr><td><i>IPSECI</i></td><td>DSW IPORT IPSECI.</td></tr><tr><td><i>IPSECO</i></td><td>DSW IPORT IPSECO.</td></tr><tr><td><i>IPTI</i></td><td>DSW IPORT IPTI.</td></tr><tr><td><i>IPTO</i></td><td>DSW IPORT IPTO.</td></tr><tr><td><i>VEP0</i></td><td>DSW IPORT VEP0.</td></tr><tr><td><i>VEP2</i></td><td>DSW IPORT VEP2.</td></tr><tr><td><i>VEP4</i></td><td>DSW IPORT VEP4.</td></tr><tr><td><i>VEP6</i></td><td>DSW IPORT VEP6.</td></tr><tr><td><i>IVS</i></td><td>DSW IPORT IVS.</td></tr><tr><td><i>L2TI1</i></td><td>DSW IPORT L2TI1.</td></tr><tr><td><i>L2TO</i></td><td>DSW IPORT L2TO.</td></tr><tr><td><i>L2TI0</i></td><td>DSW IPORT L2TI0.</td></tr><tr><td><i>PLE</i></td><td>DSW IPORT PLE.</td></tr><tr><td><i>SPATH</i></td><td>DSW IPORT SPATH.</td></tr><tr><td><i>QTM</i></td><td>DSW IPORT QTM.</td></tr></table>	Option	Description	<i>DFR</i>	DSW IPORT DFR.	<i>IPSECI</i>	DSW IPORT IPSECI.	<i>IPSECO</i>	DSW IPORT IPSECO.	<i>IPTI</i>	DSW IPORT IPTI.	<i>IPTO</i>	DSW IPORT IPTO.	<i>VEP0</i>	DSW IPORT VEP0.	<i>VEP2</i>	DSW IPORT VEP2.	<i>VEP4</i>	DSW IPORT VEP4.	<i>VEP6</i>	DSW IPORT VEP6.	<i>IVS</i>	DSW IPORT IVS.	<i>L2TI1</i>	DSW IPORT L2TI1.	<i>L2TO</i>	DSW IPORT L2TO.	<i>L2TI0</i>	DSW IPORT L2TI0.	<i>PLE</i>	DSW IPORT PLE.	<i>SPATH</i>	DSW IPORT SPATH.	<i>QTM</i>	DSW IPORT QTM.			
	Option	Description																																				
	<i>DFR</i>	DSW IPORT DFR.																																				
	<i>IPSECI</i>	DSW IPORT IPSECI.																																				
	<i>IPSECO</i>	DSW IPORT IPSECO.																																				
	<i>IPTI</i>	DSW IPORT IPTI.																																				
	<i>IPTO</i>	DSW IPORT IPTO.																																				
	<i>VEP0</i>	DSW IPORT VEP0.																																				
	<i>VEP2</i>	DSW IPORT VEP2.																																				
	<i>VEP4</i>	DSW IPORT VEP4.																																				
	<i>VEP6</i>	DSW IPORT VEP6.																																				
	<i>IVS</i>	DSW IPORT IVS.																																				
	<i>L2TI1</i>	DSW IPORT L2TI1.																																				
	<i>L2TO</i>	DSW IPORT L2TO.																																				
	<i>L2TI0</i>	DSW IPORT L2TI0.																																				
	<i>PLE</i>	DSW IPORT PLE.																																				
	<i>SPATH</i>	DSW IPORT SPATH.																																				
<i>QTM</i>	DSW IPORT QTM.																																					
oport	Set NPU DSW DTS out port.	option	-	EIF0																																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>EIF0</i></td><td>DSW OPORT EIF0.</td></tr><tr><td><i>EIF1</i></td><td>DSW OPORT EIF1.</td></tr><tr><td><i>EIF2</i></td><td>DSW OPORT EIF2.</td></tr><tr><td><i>EIF3</i></td><td>DSW OPORT EIF3.</td></tr><tr><td><i>EIF4</i></td><td>DSW OPORT EIF4.</td></tr><tr><td><i>EIF5</i></td><td>DSW OPORT EIF5.</td></tr><tr><td><i>EIF6</i></td><td>DSW OPORT EIF6.</td></tr><tr><td><i>EIF7</i></td><td>DSW OPORT EIF7.</td></tr><tr><td><i>HRX</i></td><td>DSW OPORT HRX.</td></tr><tr><td><i>SSE0</i></td><td>DSW OPORT SSE0.</td></tr></table>	Option	Description	<i>EIF0</i>	DSW OPORT EIF0.	<i>EIF1</i>	DSW OPORT EIF1.	<i>EIF2</i>	DSW OPORT EIF2.	<i>EIF3</i>	DSW OPORT EIF3.	<i>EIF4</i>	DSW OPORT EIF4.	<i>EIF5</i>	DSW OPORT EIF5.	<i>EIF6</i>	DSW OPORT EIF6.	<i>EIF7</i>	DSW OPORT EIF7.	<i>HRX</i>	DSW OPORT HRX.	<i>SSE0</i>	DSW OPORT SSE0.															
	Option	Description																																				
	<i>EIF0</i>	DSW OPORT EIF0.																																				
	<i>EIF1</i>	DSW OPORT EIF1.																																				
	<i>EIF2</i>	DSW OPORT EIF2.																																				
	<i>EIF3</i>	DSW OPORT EIF3.																																				
	<i>EIF4</i>	DSW OPORT EIF4.																																				
	<i>EIF5</i>	DSW OPORT EIF5.																																				
	<i>EIF6</i>	DSW OPORT EIF6.																																				
	<i>EIF7</i>	DSW OPORT EIF7.																																				
	<i>HRX</i>	DSW OPORT HRX.																																				
	<i>SSE0</i>	DSW OPORT SSE0.																																				

Parameter	Description	Type	Size	Default																																														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>SSE1</i></td><td>DSW OPORT SSE1.</td></tr><tr><td><i>SSE2</i></td><td>DSW OPORT SSE2.</td></tr><tr><td><i>SSE3</i></td><td>DSW OPORT SSE3.</td></tr><tr><td><i>RLT</i></td><td>DSW OPORT RLT.</td></tr><tr><td><i>DFR</i></td><td>DSW OPORT DFR.</td></tr><tr><td><i>IPSECI</i></td><td>DSW OPORT IPSECI.</td></tr><tr><td><i>IPSECO</i></td><td>DSW OPORT IPSECO.</td></tr><tr><td><i>IPTI</i></td><td>DSW OPORT IPTI.</td></tr><tr><td><i>IPTO</i></td><td>DSW OPORT IPTO.</td></tr><tr><td><i>VEP0</i></td><td>DSW OPORT VEP0.</td></tr><tr><td><i>VEP2</i></td><td>DSW OPORT VEP2.</td></tr><tr><td><i>VEP4</i></td><td>DSW OPORT VEP4.</td></tr><tr><td><i>VEP6</i></td><td>DSW OPORT VEP6.</td></tr><tr><td><i>IVS</i></td><td>DSW OPORT IVS.</td></tr><tr><td><i>L2TI1</i></td><td>DSW OPORT L2TI1.</td></tr><tr><td><i>L2TO</i></td><td>DSW OPORT L2TO.</td></tr><tr><td><i>L2TI0</i></td><td>DSW OPORT L2TI0.</td></tr><tr><td><i>PLE</i></td><td>DSW OPORT PLE.</td></tr><tr><td><i>SYNK</i></td><td>DSW OPORT SYNK.</td></tr><tr><td><i>NSS</i></td><td>DSW OPORT NSS.</td></tr><tr><td><i>TSK</i></td><td>DSW OPORT TSK.</td></tr><tr><td><i>QTM</i></td><td>DSW OPORT QTM.</td></tr></table>	Option	Description	<i>SSE1</i>	DSW OPORT SSE1.	<i>SSE2</i>	DSW OPORT SSE2.	<i>SSE3</i>	DSW OPORT SSE3.	<i>RLT</i>	DSW OPORT RLT.	<i>DFR</i>	DSW OPORT DFR.	<i>IPSECI</i>	DSW OPORT IPSECI.	<i>IPSECO</i>	DSW OPORT IPSECO.	<i>IPTI</i>	DSW OPORT IPTI.	<i>IPTO</i>	DSW OPORT IPTO.	<i>VEP0</i>	DSW OPORT VEP0.	<i>VEP2</i>	DSW OPORT VEP2.	<i>VEP4</i>	DSW OPORT VEP4.	<i>VEP6</i>	DSW OPORT VEP6.	<i>IVS</i>	DSW OPORT IVS.	<i>L2TI1</i>	DSW OPORT L2TI1.	<i>L2TO</i>	DSW OPORT L2TO.	<i>L2TI0</i>	DSW OPORT L2TI0.	<i>PLE</i>	DSW OPORT PLE.	<i>SYNK</i>	DSW OPORT SYNK.	<i>NSS</i>	DSW OPORT NSS.	<i>TSK</i>	DSW OPORT TSK.	<i>QTM</i>	DSW OPORT QTM.			
	Option	Description																																																
	<i>SSE1</i>	DSW OPORT SSE1.																																																
	<i>SSE2</i>	DSW OPORT SSE2.																																																
	<i>SSE3</i>	DSW OPORT SSE3.																																																
	<i>RLT</i>	DSW OPORT RLT.																																																
	<i>DFR</i>	DSW OPORT DFR.																																																
	<i>IPSECI</i>	DSW OPORT IPSECI.																																																
	<i>IPSECO</i>	DSW OPORT IPSECO.																																																
	<i>IPTI</i>	DSW OPORT IPTI.																																																
	<i>IPTO</i>	DSW OPORT IPTO.																																																
	<i>VEP0</i>	DSW OPORT VEP0.																																																
	<i>VEP2</i>	DSW OPORT VEP2.																																																
	<i>VEP4</i>	DSW OPORT VEP4.																																																
	<i>VEP6</i>	DSW OPORT VEP6.																																																
	<i>IVS</i>	DSW OPORT IVS.																																																
	<i>L2TI1</i>	DSW OPORT L2TI1.																																																
	<i>L2TO</i>	DSW OPORT L2TO.																																																
	<i>L2TI0</i>	DSW OPORT L2TI0.																																																
	<i>PLE</i>	DSW OPORT PLE.																																																
	<i>SYNK</i>	DSW OPORT SYNK.																																																
	<i>NSS</i>	DSW OPORT NSS.																																																
	<i>TSK</i>	DSW OPORT TSK.																																																
<i>QTM</i>	DSW OPORT QTM.																																																	
profile-id	Set NPU DSW DTS profile ID.	integer	Minimum value: 1 Maximum value: 32	0																																														
queue-select	Set NPU DSW DTS queue ID select.	integer	Minimum value: 0 Maximum value: 4095	0																																														

## config fp-anomaly

Parameter	Description	Type	Size	Default						
ipv4-ver-err *	Invalid IPv4 header version anomalies.	option	-	drop						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>drop</td><td>Drop IPv4 invalid header version.</td></tr><tr><td>trap-to-host</td><td>Forward IPv4 invalid header version to main CPU for processing.</td></tr></table>	Option	Description	drop	Drop IPv4 invalid header version.	trap-to-host	Forward IPv4 invalid header version to main CPU for processing.			
Option	Description									
drop	Drop IPv4 invalid header version.									
trap-to-host	Forward IPv4 invalid header version to main CPU for processing.									
ipv4-ihl-err *	Invalid IPv4 header length anomalies.	option	-	drop						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>drop</td><td>Drop IPv4 invalid header length.</td></tr><tr><td>trap-to-host</td><td>Forward IPv4 invalid header length to main CPU for processing.</td></tr></table>	Option	Description	drop	Drop IPv4 invalid header length.	trap-to-host	Forward IPv4 invalid header length to main CPU for processing.			
Option	Description									
drop	Drop IPv4 invalid header length.									
trap-to-host	Forward IPv4 invalid header length to main CPU for processing.									
ipv4-len-err *	Invalid IPv4 packet length anomalies.	option	-	drop						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>drop</td><td>Drop IPv4 invalid packet length.</td></tr><tr><td>trap-to-host</td><td>Forward IPv4 invalid packet length to main CPU for processing.</td></tr></table>	Option	Description	drop	Drop IPv4 invalid packet length.	trap-to-host	Forward IPv4 invalid packet length to main CPU for processing.			
Option	Description									
drop	Drop IPv4 invalid packet length.									
trap-to-host	Forward IPv4 invalid packet length to main CPU for processing.									
ipv4-ttlzero-err *	Invalid IPv4 TTL field zero anomalies.	option	-	drop						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>drop</td><td>Drop IPv4 invalid TTL field zero.</td></tr><tr><td>trap-to-host</td><td>Forward IPv4 invalid TTL field zero to main CPU for processing.</td></tr></table>	Option	Description	drop	Drop IPv4 invalid TTL field zero.	trap-to-host	Forward IPv4 invalid TTL field zero to main CPU for processing.			
Option	Description									
drop	Drop IPv4 invalid TTL field zero.									
trap-to-host	Forward IPv4 invalid TTL field zero to main CPU for processing.									
ipv4-csum-err	Invalid IPv4 packet checksum anomalies.	option	-	drop						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>drop</td><td>Drop IPv4 invalid L3 checksum.</td></tr><tr><td>trap-to-host</td><td>Forward IPv4 invalid L3 checksum to main CPU for processing.</td></tr></table>	Option	Description	drop	Drop IPv4 invalid L3 checksum.	trap-to-host	Forward IPv4 invalid L3 checksum to main CPU for processing.			
Option	Description									
drop	Drop IPv4 invalid L3 checksum.									
trap-to-host	Forward IPv4 invalid L3 checksum to main CPU for processing.									
ipv4-opt-err *	Invalid IPv4 option parsing anomalies.	option	-	drop						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>drop</td><td>Drop IPv4 invalid option parsing.</td></tr><tr><td>trap-to-host</td><td>Forward IPv4 invalid option parsing to main CPU for processing.</td></tr></table>	Option	Description	drop	Drop IPv4 invalid option parsing.	trap-to-host	Forward IPv4 invalid option parsing to main CPU for processing.			
Option	Description									
drop	Drop IPv4 invalid option parsing.									
trap-to-host	Forward IPv4 invalid option parsing to main CPU for processing.									
tcp-hlen-err *	Invalid IPv4 TCP header length anomalies.	option	-	drop						



Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>drop</i>	Drop IPv4 invalid TCP packet header length.		
	<i>trap-to-host</i>	Forward IPv4 invalid TCP packet header length to main CPU for processing.		
tcp-plen-err *	Invalid IPv4 TCP packet length anomalies.	option	-	drop
	<b>Option</b>	<b>Description</b>		
	<i>drop</i>	Drop IPv4 invalid TCP packet length.		
	<i>trap-to-host</i>	Forward IPv4 invalid TCP packet length to main CPU for processing.		
tcp-csum-err	Invalid IPv4 TCP packet checksum anomalies.	option	-	drop
	<b>Option</b>	<b>Description</b>		
	<i>drop</i>	Drop IPv4 invalid TCP packet checksum.		
	<i>trap-to-host</i>	Forward IPv4 invalid TCP packet checksum to main CPU for processing.		
udp-plen-err *	Invalid IPv4 UDP packet minimum length anomalies.	option	-	drop
	<b>Option</b>	<b>Description</b>		
	<i>drop</i>	Drop IPv4 invalid UDP packet minimum length.		
	<i>trap-to-host</i>	Forward IPv4 invalid UDP packet minimum length to main CPU for processing.		
udp-hlen-err *	Invalid IPv4 UDP packet header length anomalies.	option	-	drop
	<b>Option</b>	<b>Description</b>		
	<i>drop</i>	Drop IPv4 invalid UDP header length.		
	<i>trap-to-host</i>	Forward IPv4 invalid UDP header length to main CPU for processing.		
udp-csum-err	Invalid IPv4 UDP packet checksum anomalies.	option	-	drop
	<b>Option</b>	<b>Description</b>		
	<i>drop</i>	Drop IPv4 invalid UDP packet checksum.		
	<i>trap-to-host</i>	Forward IPv4 invalid UDP packet checksum to main CPU for processing.		
udp-len-err *	Invalid IPv4 UDP packet length anomalies.	option	-	drop
	<b>Option</b>	<b>Description</b>		
	<i>drop</i>	Drop IPv4 invalid UDP packet length.		
	<i>trap-to-host</i>	Forward IPv4 invalid UDP packet length to main CPU for processing.		

Parameter	Description	Type	Size	Default						
udplite-cover-err *	Invalid IPv4 UDP-Lite packet coverage anomalies.	option	-	drop						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>drop</td><td>Drop IPv4 invalid UDP-Lite packet coverage.</td></tr><tr><td>trap-to-host</td><td>Forward IPv4 invalid UDP-Lite packet coverage to main CPU for processing.</td></tr></table>	Option	Description	drop	Drop IPv4 invalid UDP-Lite packet coverage.	trap-to-host	Forward IPv4 invalid UDP-Lite packet coverage to main CPU for processing.			
Option	Description									
drop	Drop IPv4 invalid UDP-Lite packet coverage.									
trap-to-host	Forward IPv4 invalid UDP-Lite packet coverage to main CPU for processing.									
udplite-csum-err *	Invalid IPv4 UDP-Lite packet checksum anomalies.	option	-	drop						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>drop</td><td>Drop IPv4 invalid UDP-Lite packet checksum.</td></tr><tr><td>trap-to-host</td><td>Forward IPv4 invalid UDP-Lite packet checksum to main CPU for processing.</td></tr></table>	Option	Description	drop	Drop IPv4 invalid UDP-Lite packet checksum.	trap-to-host	Forward IPv4 invalid UDP-Lite packet checksum to main CPU for processing.			
Option	Description									
drop	Drop IPv4 invalid UDP-Lite packet checksum.									
trap-to-host	Forward IPv4 invalid UDP-Lite packet checksum to main CPU for processing.									
icmp-minlen-err *	Invalid IPv4 ICMP short packet anomalies.	option	-	drop						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>drop</td><td>Drop IPv4 invalid ICMP short packet.</td></tr><tr><td>trap-to-host</td><td>Forward IPv4 invalid ICMP short packet to main CPU for processing.</td></tr></table>	Option	Description	drop	Drop IPv4 invalid ICMP short packet.	trap-to-host	Forward IPv4 invalid ICMP short packet to main CPU for processing.			
Option	Description									
drop	Drop IPv4 invalid ICMP short packet.									
trap-to-host	Forward IPv4 invalid ICMP short packet to main CPU for processing.									
icmp-csum-err	Invalid IPv4 ICMP packet checksum anomalies.	option	-	drop						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>drop</td><td>Drop IPv4 invalid ICMP checksum.</td></tr><tr><td>trap-to-host</td><td>Forward IPv4 invalid ICMP checksum to main CPU for processing.</td></tr></table>	Option	Description	drop	Drop IPv4 invalid ICMP checksum.	trap-to-host	Forward IPv4 invalid ICMP checksum to main CPU for processing.			
Option	Description									
drop	Drop IPv4 invalid ICMP checksum.									
trap-to-host	Forward IPv4 invalid ICMP checksum to main CPU for processing.									
esp-minlen-err *	Invalid IPv4 ESP short packet anomalies.	option	-	drop						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>drop</td><td>Drop IPv4 invalid ESP short packet.</td></tr><tr><td>trap-to-host</td><td>Forward IPv4 invalid ESP short packet to main CPU for processing.</td></tr></table>	Option	Description	drop	Drop IPv4 invalid ESP short packet.	trap-to-host	Forward IPv4 invalid ESP short packet to main CPU for processing.			
Option	Description									
drop	Drop IPv4 invalid ESP short packet.									
trap-to-host	Forward IPv4 invalid ESP short packet to main CPU for processing.									
unknproto-minlen-err *	Invalid IPv4 L4 unknown protocol short packet anomalies.	option	-	drop						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>drop</td><td>Drop IPv4 invalid L4 unknown protocol short packet.</td></tr></table>	Option	Description	drop	Drop IPv4 invalid L4 unknown protocol short packet.					
Option	Description									
drop	Drop IPv4 invalid L4 unknown protocol short packet.									

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>trap-to-host</i>	Forward IPv4 invalid L4 unknown protocol short packet to main CPU for processing.		
ipv6-ver-err *	Invalid IPv6 packet version anomalies.	option	-	drop
	<b>Option</b>	<b>Description</b>		
	<i>drop</i>	Drop IPv6 with invalid packet version.		
	<i>trap-to-host</i>	Forward IPv6 with invalid packet version to FortiOS.		
ipv6-ihl-err *	Invalid IPv6 packet length anomalies.	option	-	drop
	<b>Option</b>	<b>Description</b>		
	<i>drop</i>	Drop IPv6 with invalid packet length.		
	<i>trap-to-host</i>	Forward IPv6 with invalid packet length to FortiOS.		
ipv6-plen-zero *	Invalid IPv6 packet payload length zero anomalies.	option	-	drop
	<b>Option</b>	<b>Description</b>		
	<i>drop</i>	Drop IPv6 with invalid packet payload length zero.		
	<i>trap-to-host</i>	Forward IPv6 with invalid packet payload length zero to FortiOS.		
ipv6-exthdr-order-err *	Invalid IPv6 packet extension header ordering anomalies.	option	-	drop
	<b>Option</b>	<b>Description</b>		
	<i>drop</i>	Drop IPv6 with invalid packet extension header ordering.		
	<i>trap-to-host</i>	Forward IPv6 with invalid packet extension header ordering to FortiOS.		
ipv6-exthdr-len-err *	Invalid IPv6 packet chain extension header total length anomalies.	option	-	drop
	<b>Option</b>	<b>Description</b>		
	<i>drop</i>	Drop IPv6 with invalid packet chain extension header total length.		
	<i>trap-to-host</i>	Forward IPv6 with invalid packet chain extension header total length to FortiOS.		

\* This parameter may not exist in some models.

## config hpe

Parameter	Description	Type	Size	Default
all-protocol	Maximum packet rate of each host queue except high priority traffic, set 0 to disable.	integer	Minimum value: 0 Maximum value: 32000000	400000
tcpsyn-max	Maximum TCP SYN packet rate.	integer	Minimum value: 1000 Maximum value: 32000000	40000
tcpsyn-ack-max	Maximum TCP carries SYN and ACK flags packet rate.	integer	Minimum value: 1000 Maximum value: 32000000	40000
tcpfin-rst-max	Maximum TCP carries FIN or RST flags packet rate.	integer	Minimum value: 1000 Maximum value: 32000000	40000
tcp-max	Maximum TCP packet rate.	integer	Minimum value: 1000 Maximum value: 32000000	40000
udp-max	Maximum UDP packet rate.	integer	Minimum value: 1000 Maximum value: 32000000	40000
icmp-max	Maximum ICMP packet rate.	integer	Minimum value: 1000 Maximum value: 32000000	5000
sctp-max	Maximum SCTP packet rate.	integer	Minimum value: 1000 Maximum value: 32000000	5000

Parameter	Description	Type	Size	Default						
esp-max	Maximum ESP packet rate.	integer	Minimum value: 1000 Maximum value: 32000000	5000						
ip-frag-max	Maximum fragmented IP packet rate.	integer	Minimum value: 1000 Maximum value: 32000000	5000						
ip-others-max	Maximum IP packet rate for other packets.	integer	Minimum value: 1000 Maximum value: 32000000	5000						
arp-max	Maximum ARP packet rate.	integer	Minimum value: 1000 Maximum value: 32000000	5000						
l2-others-max	Maximum L2 packet rate for L2 packets that are not ARP packets.	integer	Minimum value: 1000 Maximum value: 32000000	5000						
high-priority	Maximum packet rate for high priority traffic packets.	integer	Minimum value: 1000 Maximum value: 32000000	400000						
enable-shaper	Enable/Disable NPU Host Protection Engine (HPE) for packet type shaper.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable NPU HPE shaping based on packet type.</td></tr><tr><td>enable</td><td>Enable NPU HPE shaping based on packet type.</td></tr></table>	Option	Description	disable	Disable NPU HPE shaping based on packet type.	enable	Enable NPU HPE shaping based on packet type.			
Option	Description									
disable	Disable NPU HPE shaping based on packet type.									
enable	Enable NPU HPE shaping based on packet type.									

## config ip-reassembly

Parameter	Description	Type	Size	Default						
min-timeout	Minimum timeout value for IP reassembly (5 us - 600,000,000 us).	integer	Minimum value: 5 Maximum value: 600000000	64						
max-timeout	Maximum timeout value for IP reassembly (5 us - 600,000,000 us).	integer	Minimum value: 5 Maximum value: 600000000	200000						
status	Set IP reassembly processing status.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable IP reassembly.</td></tr><tr><td><i>enable</i></td><td>Enable IP reassembly.</td></tr></table>				Option	Description	<i>disable</i>	Disable IP reassembly.	<i>enable</i>	Enable IP reassembly.
Option	Description									
<i>disable</i>	Disable IP reassembly.									
<i>enable</i>	Enable IP reassembly.									

## config isf-np-queues

Parameter	Description	Type	Size	Default
cos0	CoS profile name for CoS 0.	string	Maximum length: 35	
cos1	CoS profile name for CoS 1.	string	Maximum length: 35	
cos2	CoS profile name for CoS 2.	string	Maximum length: 35	
cos3	CoS profile name for CoS 3.	string	Maximum length: 35	
cos4	CoS profile name for CoS 4.	string	Maximum length: 35	
cos5	CoS profile name for CoS 5.	string	Maximum length: 35	
cos6	CoS profile name for CoS 6.	string	Maximum length: 35	
cos7	CoS profile name for CoS 7.	string	Maximum length: 35	

## config profile

Parameter	Description	Type	Size	Default
id	Profile ID.	integer	Minimum value: 0 Maximum value: 255	0
type	Profile type.	option	-	cos
	Option	Description		
	cos	VLAN priority.		
	dscp	IP differentiated services code point.		
weight	Class weight.	integer	Minimum value: 0 Maximum value: 15	6
cos0	Queue number of CoS 0.	option	-	queue0
	Option	Description		
	queue0	Queue number 0.		
	queue1	Queue number 1.		
	queue2	Queue number 2.		
	queue3	Queue number 3.		
	queue4	Queue number 4.		
	queue5	Queue number 5.		
	queue6	Queue number 6.		
	queue7	Queue number 7.		
cos1	Queue number of CoS 1.	option	-	queue1
	Option	Description		
	queue0	Queue number 0.		
	queue1	Queue number 1.		
	queue2	Queue number 2.		
	queue3	Queue number 3.		
	queue4	Queue number 4.		
	queue5	Queue number 5.		

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
cos2	Queue number of CoS 2.	option	-	queue2
	<b>Option</b>	<b>Description</b>		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
cos3	Queue number of CoS 3.	option	-	queue3
	<b>Option</b>	<b>Description</b>		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
cos4	Queue number of CoS 4.	option	-	queue4
	<b>Option</b>	<b>Description</b>		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		



Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
cos5	Queue number of CoS 5.	option	-	queue5
	<b>Option</b>	<b>Description</b>		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
cos6	Queue number of CoS 6.	option	-	queue6
	<b>Option</b>	<b>Description</b>		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
cos7	Queue number of CoS 7.	option	-	queue7

Parameter	Description	Type	Size	Default																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>queue0</i></td><td>Queue number 0.</td></tr><tr><td><i>queue1</i></td><td>Queue number 1.</td></tr><tr><td><i>queue2</i></td><td>Queue number 2.</td></tr><tr><td><i>queue3</i></td><td>Queue number 3.</td></tr><tr><td><i>queue4</i></td><td>Queue number 4.</td></tr><tr><td><i>queue5</i></td><td>Queue number 5.</td></tr><tr><td><i>queue6</i></td><td>Queue number 6.</td></tr><tr><td><i>queue7</i></td><td>Queue number 7.</td></tr></table>	Option	Description	<i>queue0</i>	Queue number 0.	<i>queue1</i>	Queue number 1.	<i>queue2</i>	Queue number 2.	<i>queue3</i>	Queue number 3.	<i>queue4</i>	Queue number 4.	<i>queue5</i>	Queue number 5.	<i>queue6</i>	Queue number 6.	<i>queue7</i>	Queue number 7.			
	Option	Description																				
	<i>queue0</i>	Queue number 0.																				
	<i>queue1</i>	Queue number 1.																				
	<i>queue2</i>	Queue number 2.																				
	<i>queue3</i>	Queue number 3.																				
	<i>queue4</i>	Queue number 4.																				
	<i>queue5</i>	Queue number 5.																				
	<i>queue6</i>	Queue number 6.																				
<i>queue7</i>	Queue number 7.																					
dscp0	Queue number of DSCP 0.	option	-	queue0																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>queue0</i></td><td>Queue number 0.</td></tr><tr><td><i>queue1</i></td><td>Queue number 1.</td></tr><tr><td><i>queue2</i></td><td>Queue number 2.</td></tr><tr><td><i>queue3</i></td><td>Queue number 3.</td></tr><tr><td><i>queue4</i></td><td>Queue number 4.</td></tr><tr><td><i>queue5</i></td><td>Queue number 5.</td></tr><tr><td><i>queue6</i></td><td>Queue number 6.</td></tr><tr><td><i>queue7</i></td><td>Queue number 7.</td></tr></table>	Option	Description	<i>queue0</i>	Queue number 0.	<i>queue1</i>	Queue number 1.	<i>queue2</i>	Queue number 2.	<i>queue3</i>	Queue number 3.	<i>queue4</i>	Queue number 4.	<i>queue5</i>	Queue number 5.	<i>queue6</i>	Queue number 6.	<i>queue7</i>	Queue number 7.			
	Option	Description																				
	<i>queue0</i>	Queue number 0.																				
	<i>queue1</i>	Queue number 1.																				
	<i>queue2</i>	Queue number 2.																				
	<i>queue3</i>	Queue number 3.																				
	<i>queue4</i>	Queue number 4.																				
	<i>queue5</i>	Queue number 5.																				
	<i>queue6</i>	Queue number 6.																				
<i>queue7</i>	Queue number 7.																					
dscp1	Queue number of DSCP 1.	option	-	queue1																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>queue0</i></td><td>Queue number 0.</td></tr><tr><td><i>queue1</i></td><td>Queue number 1.</td></tr><tr><td><i>queue2</i></td><td>Queue number 2.</td></tr><tr><td><i>queue3</i></td><td>Queue number 3.</td></tr><tr><td><i>queue4</i></td><td>Queue number 4.</td></tr><tr><td><i>queue5</i></td><td>Queue number 5.</td></tr><tr><td><i>queue6</i></td><td>Queue number 6.</td></tr><tr><td><i>queue7</i></td><td>Queue number 7.</td></tr></table>	Option	Description	<i>queue0</i>	Queue number 0.	<i>queue1</i>	Queue number 1.	<i>queue2</i>	Queue number 2.	<i>queue3</i>	Queue number 3.	<i>queue4</i>	Queue number 4.	<i>queue5</i>	Queue number 5.	<i>queue6</i>	Queue number 6.	<i>queue7</i>	Queue number 7.			
	Option	Description																				
	<i>queue0</i>	Queue number 0.																				
	<i>queue1</i>	Queue number 1.																				
	<i>queue2</i>	Queue number 2.																				
	<i>queue3</i>	Queue number 3.																				
	<i>queue4</i>	Queue number 4.																				
	<i>queue5</i>	Queue number 5.																				
	<i>queue6</i>	Queue number 6.																				
<i>queue7</i>	Queue number 7.																					

Parameter	Description	Type	Size	Default
dscp2	Queue number of DSCP 2.	option	-	queue2
	<b>Option</b>	<b>Description</b>		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
dscp3	Queue number of DSCP 3.	option	-	queue3
	<b>Option</b>	<b>Description</b>		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
dscp4	Queue number of DSCP 4.	option	-	queue4
	<b>Option</b>	<b>Description</b>		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>queue7</i>	Queue number 7.		
dscp5	Queue number of DSCP 5.	option	-	queue5
	<b>Option</b>	<b>Description</b>		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
dscp6	Queue number of DSCP 6.	option	-	queue6
	<b>Option</b>	<b>Description</b>		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
dscp7	Queue number of DSCP 7.	option	-	queue7
	<b>Option</b>	<b>Description</b>		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
dscp8	Queue number of DSCP 8.	option	-	queue0
	<b>Option</b>	<b>Description</b>		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
dscp9	Queue number of DSCP 9.	option	-	queue1
	<b>Option</b>	<b>Description</b>		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
dscp10	Queue number of DSCP 10.	option	-	queue2
	<b>Option</b>	<b>Description</b>		
	<i>queue0</i>	Queue number 0.		

Parameter	Description	Type	Size	Default																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>queue1</i></td><td>Queue number 1.</td></tr><tr><td><i>queue2</i></td><td>Queue number 2.</td></tr><tr><td><i>queue3</i></td><td>Queue number 3.</td></tr><tr><td><i>queue4</i></td><td>Queue number 4.</td></tr><tr><td><i>queue5</i></td><td>Queue number 5.</td></tr><tr><td><i>queue6</i></td><td>Queue number 6.</td></tr><tr><td><i>queue7</i></td><td>Queue number 7.</td></tr></table>	Option	Description	<i>queue1</i>	Queue number 1.	<i>queue2</i>	Queue number 2.	<i>queue3</i>	Queue number 3.	<i>queue4</i>	Queue number 4.	<i>queue5</i>	Queue number 5.	<i>queue6</i>	Queue number 6.	<i>queue7</i>	Queue number 7.					
	Option	Description																				
	<i>queue1</i>	Queue number 1.																				
	<i>queue2</i>	Queue number 2.																				
	<i>queue3</i>	Queue number 3.																				
	<i>queue4</i>	Queue number 4.																				
	<i>queue5</i>	Queue number 5.																				
	<i>queue6</i>	Queue number 6.																				
<i>queue7</i>	Queue number 7.																					
dscp11	Queue number of DSCP 11.	option	-	queue3																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>queue0</i></td><td>Queue number 0.</td></tr><tr><td><i>queue1</i></td><td>Queue number 1.</td></tr><tr><td><i>queue2</i></td><td>Queue number 2.</td></tr><tr><td><i>queue3</i></td><td>Queue number 3.</td></tr><tr><td><i>queue4</i></td><td>Queue number 4.</td></tr><tr><td><i>queue5</i></td><td>Queue number 5.</td></tr><tr><td><i>queue6</i></td><td>Queue number 6.</td></tr><tr><td><i>queue7</i></td><td>Queue number 7.</td></tr></table>	Option	Description	<i>queue0</i>	Queue number 0.	<i>queue1</i>	Queue number 1.	<i>queue2</i>	Queue number 2.	<i>queue3</i>	Queue number 3.	<i>queue4</i>	Queue number 4.	<i>queue5</i>	Queue number 5.	<i>queue6</i>	Queue number 6.	<i>queue7</i>	Queue number 7.			
	Option	Description																				
	<i>queue0</i>	Queue number 0.																				
	<i>queue1</i>	Queue number 1.																				
	<i>queue2</i>	Queue number 2.																				
	<i>queue3</i>	Queue number 3.																				
	<i>queue4</i>	Queue number 4.																				
	<i>queue5</i>	Queue number 5.																				
<i>queue6</i>	Queue number 6.																					
<i>queue7</i>	Queue number 7.																					
dscp12	Queue number of DSCP 12.	option	-	queue4																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>queue0</i></td><td>Queue number 0.</td></tr><tr><td><i>queue1</i></td><td>Queue number 1.</td></tr><tr><td><i>queue2</i></td><td>Queue number 2.</td></tr><tr><td><i>queue3</i></td><td>Queue number 3.</td></tr><tr><td><i>queue4</i></td><td>Queue number 4.</td></tr><tr><td><i>queue5</i></td><td>Queue number 5.</td></tr><tr><td><i>queue6</i></td><td>Queue number 6.</td></tr><tr><td><i>queue7</i></td><td>Queue number 7.</td></tr></table>	Option	Description	<i>queue0</i>	Queue number 0.	<i>queue1</i>	Queue number 1.	<i>queue2</i>	Queue number 2.	<i>queue3</i>	Queue number 3.	<i>queue4</i>	Queue number 4.	<i>queue5</i>	Queue number 5.	<i>queue6</i>	Queue number 6.	<i>queue7</i>	Queue number 7.			
	Option	Description																				
	<i>queue0</i>	Queue number 0.																				
	<i>queue1</i>	Queue number 1.																				
	<i>queue2</i>	Queue number 2.																				
	<i>queue3</i>	Queue number 3.																				
	<i>queue4</i>	Queue number 4.																				
	<i>queue5</i>	Queue number 5.																				
<i>queue6</i>	Queue number 6.																					
<i>queue7</i>	Queue number 7.																					
dscp13	Queue number of DSCP 13.	option	-	queue5																		

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
dscp14	Queue number of DSCP 14.	option	-	queue6
	<b>Option</b>	<b>Description</b>		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
dscp15	Queue number of DSCP 15.	option	-	queue7
	<b>Option</b>	<b>Description</b>		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		

Parameter	Description	Type	Size	Default
dscp16	Queue number of DSCP 16.	option	-	queue0
	<b>Option</b>	<b>Description</b>		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
dscp17	Queue number of DSCP 17.	option	-	queue1
	<b>Option</b>	<b>Description</b>		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
dscp18	Queue number of DSCP 18.	option	-	queue2
	<b>Option</b>	<b>Description</b>		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		



Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>queue7</i>	Queue number 7.		
dscp19	Queue number of DSCP 19.	option	-	queue3
	<b>Option</b>	<b>Description</b>		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
dscp20	Queue number of DSCP 20.	option	-	queue4
	<b>Option</b>	<b>Description</b>		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
dscp21	Queue number of DSCP 21.	option	-	queue5
	<b>Option</b>	<b>Description</b>		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
dscp22	Queue number of DSCP 22.	option	-	queue6
	<b>Option</b>	<b>Description</b>		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
dscp23	Queue number of DSCP 23.	option	-	queue7
	<b>Option</b>	<b>Description</b>		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
dscp24	Queue number of DSCP 24.	option	-	queue0
	<b>Option</b>	<b>Description</b>		
	<i>queue0</i>	Queue number 0.		

Parameter	Description	Type	Size	Default																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>queue1</i></td><td>Queue number 1.</td></tr><tr><td><i>queue2</i></td><td>Queue number 2.</td></tr><tr><td><i>queue3</i></td><td>Queue number 3.</td></tr><tr><td><i>queue4</i></td><td>Queue number 4.</td></tr><tr><td><i>queue5</i></td><td>Queue number 5.</td></tr><tr><td><i>queue6</i></td><td>Queue number 6.</td></tr><tr><td><i>queue7</i></td><td>Queue number 7.</td></tr></table>	Option	Description	<i>queue1</i>	Queue number 1.	<i>queue2</i>	Queue number 2.	<i>queue3</i>	Queue number 3.	<i>queue4</i>	Queue number 4.	<i>queue5</i>	Queue number 5.	<i>queue6</i>	Queue number 6.	<i>queue7</i>	Queue number 7.					
	Option	Description																				
	<i>queue1</i>	Queue number 1.																				
	<i>queue2</i>	Queue number 2.																				
	<i>queue3</i>	Queue number 3.																				
	<i>queue4</i>	Queue number 4.																				
	<i>queue5</i>	Queue number 5.																				
	<i>queue6</i>	Queue number 6.																				
<i>queue7</i>	Queue number 7.																					
dscp25	Queue number of DSCP 25.	option	-	queue1																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>queue0</i></td><td>Queue number 0.</td></tr><tr><td><i>queue1</i></td><td>Queue number 1.</td></tr><tr><td><i>queue2</i></td><td>Queue number 2.</td></tr><tr><td><i>queue3</i></td><td>Queue number 3.</td></tr><tr><td><i>queue4</i></td><td>Queue number 4.</td></tr><tr><td><i>queue5</i></td><td>Queue number 5.</td></tr><tr><td><i>queue6</i></td><td>Queue number 6.</td></tr><tr><td><i>queue7</i></td><td>Queue number 7.</td></tr></table>	Option	Description	<i>queue0</i>	Queue number 0.	<i>queue1</i>	Queue number 1.	<i>queue2</i>	Queue number 2.	<i>queue3</i>	Queue number 3.	<i>queue4</i>	Queue number 4.	<i>queue5</i>	Queue number 5.	<i>queue6</i>	Queue number 6.	<i>queue7</i>	Queue number 7.			
	Option	Description																				
	<i>queue0</i>	Queue number 0.																				
	<i>queue1</i>	Queue number 1.																				
	<i>queue2</i>	Queue number 2.																				
	<i>queue3</i>	Queue number 3.																				
	<i>queue4</i>	Queue number 4.																				
	<i>queue5</i>	Queue number 5.																				
<i>queue6</i>	Queue number 6.																					
<i>queue7</i>	Queue number 7.																					
dscp26	Queue number of DSCP 26.	option	-	queue2																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>queue0</i></td><td>Queue number 0.</td></tr><tr><td><i>queue1</i></td><td>Queue number 1.</td></tr><tr><td><i>queue2</i></td><td>Queue number 2.</td></tr><tr><td><i>queue3</i></td><td>Queue number 3.</td></tr><tr><td><i>queue4</i></td><td>Queue number 4.</td></tr><tr><td><i>queue5</i></td><td>Queue number 5.</td></tr><tr><td><i>queue6</i></td><td>Queue number 6.</td></tr><tr><td><i>queue7</i></td><td>Queue number 7.</td></tr></table>	Option	Description	<i>queue0</i>	Queue number 0.	<i>queue1</i>	Queue number 1.	<i>queue2</i>	Queue number 2.	<i>queue3</i>	Queue number 3.	<i>queue4</i>	Queue number 4.	<i>queue5</i>	Queue number 5.	<i>queue6</i>	Queue number 6.	<i>queue7</i>	Queue number 7.			
	Option	Description																				
	<i>queue0</i>	Queue number 0.																				
	<i>queue1</i>	Queue number 1.																				
	<i>queue2</i>	Queue number 2.																				
	<i>queue3</i>	Queue number 3.																				
	<i>queue4</i>	Queue number 4.																				
	<i>queue5</i>	Queue number 5.																				
<i>queue6</i>	Queue number 6.																					
<i>queue7</i>	Queue number 7.																					
dscp27	Queue number of DSCP 27.	option	-	queue3																		

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
dscp28	Queue number of DSCP 28.	option	-	queue4
	<b>Option</b>	<b>Description</b>		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
dscp29	Queue number of DSCP 29.	option	-	queue5
	<b>Option</b>	<b>Description</b>		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		

Parameter	Description	Type	Size	Default
dscp30	Queue number of DSCP 30.	option	-	queue6
	<b>Option</b>	<b>Description</b>		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
dscp31	Queue number of DSCP 31.	option	-	queue7
	<b>Option</b>	<b>Description</b>		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
dscp32	Queue number of DSCP 32.	option	-	queue0
	<b>Option</b>	<b>Description</b>		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>queue7</i>	Queue number 7.		
dscp33	Queue number of DSCP 33.	option	-	queue1
	<b>Option</b>	<b>Description</b>		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
dscp34	Queue number of DSCP 34.	option	-	queue2
	<b>Option</b>	<b>Description</b>		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
dscp35	Queue number of DSCP 35.	option	-	queue3
	<b>Option</b>	<b>Description</b>		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
dscp36	Queue number of DSCP 36.	option	-	queue4
	<b>Option</b>	<b>Description</b>		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
dscp37	Queue number of DSCP 37.	option	-	queue5
	<b>Option</b>	<b>Description</b>		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
dscp38	Queue number of DSCP 38.	option	-	queue6
	<b>Option</b>	<b>Description</b>		
	<i>queue0</i>	Queue number 0.		

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
dscp39	Queue number of DSCP 39.	option	-	queue7
	<b>Option</b>	<b>Description</b>		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
dscp40	Queue number of DSCP 40.	option	-	queue0
	<b>Option</b>	<b>Description</b>		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
dscp41	Queue number of DSCP 41.	option	-	queue1



Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
dscp42	Queue number of DSCP 42.	option	-	queue2
	<b>Option</b>	<b>Description</b>		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
dscp43	Queue number of DSCP 43.	option	-	queue3
	<b>Option</b>	<b>Description</b>		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		

Parameter	Description	Type	Size	Default
dscp44	Queue number of DSCP 44.	option	-	queue4
	<b>Option</b>	<b>Description</b>		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
dscp45	Queue number of DSCP 45.	option	-	queue5
	<b>Option</b>	<b>Description</b>		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
dscp46	Queue number of DSCP 46.	option	-	queue6
	<b>Option</b>	<b>Description</b>		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>queue7</i>	Queue number 7.		
dscp47	Queue number of DSCP 47.	option	-	queue7
	<b>Option</b>	<b>Description</b>		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
dscp48	Queue number of DSCP 48.	option	-	queue0
	<b>Option</b>	<b>Description</b>		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
dscp49	Queue number of DSCP 49.	option	-	queue1
	<b>Option</b>	<b>Description</b>		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
dscp50	Queue number of DSCP 50.	option	-	queue2
	<b>Option</b>	<b>Description</b>		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
dscp51	Queue number of DSCP 51.	option	-	queue3
	<b>Option</b>	<b>Description</b>		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
dscp52	Queue number of DSCP 52.	option	-	queue4
	<b>Option</b>	<b>Description</b>		
	<i>queue0</i>	Queue number 0.		

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
dscp53	Queue number of DSCP 53.	option	-	queue5
	<b>Option</b>	<b>Description</b>		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
dscp54	Queue number of DSCP 54.	option	-	queue6
	<b>Option</b>	<b>Description</b>		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
dscp55	Queue number of DSCP 55.	option	-	queue7

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
dscp56	Queue number of DSCP 56.	option	-	queue0
	<b>Option</b>	<b>Description</b>		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
dscp57	Queue number of DSCP 57.	option	-	queue1
	<b>Option</b>	<b>Description</b>		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		

Parameter	Description	Type	Size	Default
dscp58	Queue number of DSCP 58.	option	-	queue2
	<b>Option</b>	<b>Description</b>		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
dscp59	Queue number of DSCP 59.	option	-	queue3
	<b>Option</b>	<b>Description</b>		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
dscp60	Queue number of DSCP 60.	option	-	queue4
	<b>Option</b>	<b>Description</b>		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>queue7</i>	Queue number 7.		
dscp61	Queue number of DSCP 61.	option	-	queue5
	<b>Option</b>	<b>Description</b>		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
dscp62	Queue number of DSCP 62.	option	-	queue6
	<b>Option</b>	<b>Description</b>		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		
dscp63	Queue number of DSCP 63.	option	-	queue7
	<b>Option</b>	<b>Description</b>		
	<i>queue0</i>	Queue number 0.		
	<i>queue1</i>	Queue number 1.		
	<i>queue2</i>	Queue number 2.		
	<i>queue3</i>	Queue number 3.		



Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>queue4</i>	Queue number 4.		
	<i>queue5</i>	Queue number 5.		
	<i>queue6</i>	Queue number 6.		
	<i>queue7</i>	Queue number 7.		

### config ethernet-type

Parameter	Description	Type	Size	Default
name	Ethernet Type Name.	string	Maximum length: 35	
type	Ethernet Type.	ether-type	Not Specified	0
queue	Queue Number.	integer	Minimum value: 0 Maximum value: 11	0
weight	Class Weight.	integer	Minimum value: 0 Maximum value: 15	15

### config ip-protocol

Parameter	Description	Type	Size	Default
name	IP Protocol Name.	string	Maximum length: 35	
protocol	IP Protocol.	integer	Minimum value: 0 Maximum value: 255	0
queue	Queue Number.	integer	Minimum value: 0 Maximum value: 11	0
weight	Class Weight.	integer	Minimum value: 0 Maximum value: 15	14

## config ip-service

Parameter	Description	Type	Size	Default
name	IP service name.	string	Maximum length: 35	
protocol	IP protocol.	integer	Minimum value: 0 Maximum value: 255	0
sport	Source port.	integer	Minimum value: 0 Maximum value: 65535	0
dport	Destination port.	integer	Minimum value: 0 Maximum value: 65535	0
queue	Queue number.	integer	Minimum value: 0 Maximum value: 11	0
weight	Class weight.	integer	Minimum value: 0 Maximum value: 15	13

## config scheduler

Parameter	Description	Type	Size	Default
name	Scheduler name.	string	Maximum length: 35	
mode	Scheduler mode.	option	-	none
	Option	Description		
	<i>none</i>	Disable QoS on NP7.		
	<i>priority</i>	Priority Based.		
	<i>round-robin</i>	Round Robin Scheduler.		

### config port-cpu-map

Parameter	Description	Type	Size	Default
interface	The interface to map to a CPU core.	string	Maximum length: 15	
cpu-core	The CPU core to map to an interface.	string	Maximum length: 31	all

### config port-npu-map

Parameter	Description	Type	Size	Default
interface	Set NPU interface port for NPU group mapping.	string	Maximum length: 15	
npu-group-index	Mapping NPU group index.	integer	Minimum value: 0 Maximum value: 4294967295	0

### config port-path-option

Parameter	Description	Type	Size	Default
ports-using-npu <interface-name>	Set ha/aux ports to handle traffic with NPU (otherwise traffic goes to Intel-NIC and then CPU). Available interfaces for NPU path.	string	Maximum length: 15	

### config priority-protocol

Parameter	Description	Type	Size	Default
bgp	Enable/disable NPU BGP priority protocol.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable NPU BGP priority protocol.		
	<i>disable</i>	Disable NPU BGP priority protocol.		
slbc	Enable/disable NPU SLBC priority protocol.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable NPU SLBC priority protocol.		
	<i>disable</i>	Disable NPU SLBC priority protocol.		

Parameter	Description	Type	Size	Default
bfd	Enable/disable NPU BFD priority protocol.	option	-	enable
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Enable NPU BFD priority protocol.		
	<i>disable</i>	Disable NPU BFD priority protocol.		

### config sse-ha-scan

Parameter	Description	Type	Size	Default
gap	Scanning message gap	integer	Minimum value: 0 Maximum value: 32767	6000

### config sw-eh-hash

Parameter	Description	Type	Size	Default
computation	Set hashing computation.	option	-	xor16
	<b>Option</b> <b>Description</b>			
	<i>xor16</i>	Use XOR operator to make 16 bits hash.		
	<i>xor8</i>	Use XOR operator to make 8 bits hash.		
	<i>xor4</i>	Use XOR operator to make 4 bits hash.		
	<i>crc16</i>	Use CRC-16-CCITT polynomial to make 16 bits hash.		
ip-protocol	Include/exclude IP protocol.	option	-	include
	<b>Option</b> <b>Description</b>			
	<i>include</i>	Include IP protocol.		
	<i>exclude</i>	Exclude IP protocol.		
source-ip-upper-16	Include/exclude source IP address upper 16 bits.	option	-	include
	<b>Option</b> <b>Description</b>			
	<i>include</i>	Include source IP address upper 16 bits.		
	<i>exclude</i>	Exclude source IP address upper 16 bits.		

Parameter	Description	Type	Size	Default						
source-ip-lower-16	Include/exclude source IP address lower 16 bits.	option	-	include						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>include</i></td><td>Include source IP address lower 16 bits.</td></tr><tr><td><i>exclude</i></td><td>Exclude source IP address lower 16 bits.</td></tr></table>	Option	Description	<i>include</i>	Include source IP address lower 16 bits.	<i>exclude</i>	Exclude source IP address lower 16 bits.			
Option	Description									
<i>include</i>	Include source IP address lower 16 bits.									
<i>exclude</i>	Exclude source IP address lower 16 bits.									
destination-ip-upper-16	Include/exclude destination IP address upper 16 bits.	option	-	include						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>include</i></td><td>Include destination IP address upper 16 bits.</td></tr><tr><td><i>exclude</i></td><td>Exclude destination IP address upper 16 bits.</td></tr></table>	Option	Description	<i>include</i>	Include destination IP address upper 16 bits.	<i>exclude</i>	Exclude destination IP address upper 16 bits.			
Option	Description									
<i>include</i>	Include destination IP address upper 16 bits.									
<i>exclude</i>	Exclude destination IP address upper 16 bits.									
destination-ip-lower-16	Include/exclude destination IP address lower 16 bits.	option	-	include						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>include</i></td><td>Include destination IP address lower 16 bits.</td></tr><tr><td><i>exclude</i></td><td>Exclude destination IP address lower 16 bits.</td></tr></table>	Option	Description	<i>include</i>	Include destination IP address lower 16 bits.	<i>exclude</i>	Exclude destination IP address lower 16 bits.			
Option	Description									
<i>include</i>	Include destination IP address lower 16 bits.									
<i>exclude</i>	Exclude destination IP address lower 16 bits.									
source-port	Include/exclude source port if TCP/UDP.	option	-	include						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>include</i></td><td>Include source port if TCP/UDP.</td></tr><tr><td><i>exclude</i></td><td>Exclude source port if TCP/UDP.</td></tr></table>	Option	Description	<i>include</i>	Include source port if TCP/UDP.	<i>exclude</i>	Exclude source port if TCP/UDP.			
Option	Description									
<i>include</i>	Include source port if TCP/UDP.									
<i>exclude</i>	Exclude source port if TCP/UDP.									
destination-port	Include/exclude destination port if TCP/UDP.	option	-	include						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>include</i></td><td>Include destination port if TCP/UDP.</td></tr><tr><td><i>exclude</i></td><td>Exclude destination port if TCP/UDP.</td></tr></table>	Option	Description	<i>include</i>	Include destination port if TCP/UDP.	<i>exclude</i>	Exclude destination port if TCP/UDP.			
Option	Description									
<i>include</i>	Include destination port if TCP/UDP.									
<i>exclude</i>	Exclude destination port if TCP/UDP.									
netmask-length	Network mask length.	integer	Minimum value: 17 Maximum value: 32	32						

## config tcp-timeout-profile

Parameter	Description	Type	Size	Default
id	Timeout profile ID	integer	Minimum value: 5 Maximum value: 47	0
tcp-idle	Set TCP establish timeout(seconds)	integer	Minimum value: 1 Maximum value: 86400	3600
fin-wait	Set fin-wait timeout(seconds)	integer	Minimum value: 1 Maximum value: 86400	120
close-wait	Set close-wait timeout(seconds)	integer	Minimum value: 1 Maximum value: 86400	120
time-wait	Set time-wait timeout(seconds)	integer	Minimum value: 1 Maximum value: 300	1
syn-sent	Set syn-sent timeout(seconds)	integer	Minimum value: 1 Maximum value: 86400	10
syn-wait	Set syn-wait timeout(seconds)	integer	Minimum value: 1 Maximum value: 86400	10

## config udp-timeout-profile

Parameter	Description	Type	Size	Default
id	Timeout profile ID	integer	Minimum value: 5 Maximum value: 63	0

Parameter	Description	Type	Size	Default
udp-idle	Set UDP idle timeout(seconds)	integer	Minimum value: 1 Maximum value: 86400	180

## config system ntp

Configure system NTP information.

```
config system ntp
    Description: Configure system NTP information.
    set authentication [enable|disable]
    set interface <interface-name1>, <interface-name2>, ...
    set key {password}
    set key-id {integer}
    set key-type [MD5|SHA1]
    config ntpserver
        Description: Configure the FortiGate to connect to any available third-party NTP
server.
        edit <id>
            set server {string}
            set ntpv3 [enable|disable]
            set authentication [enable|disable]
            set key {password}
            set key-id {integer}
            set interface-select-method [auto|sdwan|...]
            set interface {string}
        next
    end
    set ntpsync [enable|disable]
    set server-mode [enable|disable]
    set source-ip {ipv4-address}
    set source-ip6 {ipv6-address}
    set syncinterval {integer}
    set type [fortiguard|custom]
end
```

## config system ntp

Parameter	Description	Type	Size	Default						
authentication	Enable/disable authentication.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable authentication.</td></tr><tr><td><i>disable</i></td><td>Disable authentication.</td></tr></table>				Option	Description	<i>enable</i>	Enable authentication.	<i>disable</i>	Disable authentication.
Option	Description									
<i>enable</i>	Enable authentication.									
<i>disable</i>	Disable authentication.									

Parameter	Description	Type	Size	Default						
interface <interface-name>	FortiGate interface(s) with NTP server mode enabled. Devices on your network can contact these interfaces for NTP services. Interface name.	string	Maximum length: 79							
key	Key for authentication.	password	Not Specified							
key-id	Key ID for authentication.	integer	Minimum value: 0 Maximum value: 4294967295	0						
key-type	Key type for authentication (MD5, SHA1).	option	-	MD5						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>MD5</td><td>Use MD5 to authenticate the message.</td></tr><tr><td>SHA1</td><td>Use SHA1 to authenticate the message.</td></tr></table>				Option	Description	MD5	Use MD5 to authenticate the message.	SHA1	Use SHA1 to authenticate the message.
Option	Description									
MD5	Use MD5 to authenticate the message.									
SHA1	Use SHA1 to authenticate the message.									
ntpsync	Enable/disable setting the FortiGate system time by synchronizing with an NTP Server.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable synchronization with NTP Server.</td></tr><tr><td>disable</td><td>Disable synchronization with NTP Server.</td></tr></table>				Option	Description	enable	Enable synchronization with NTP Server.	disable	Disable synchronization with NTP Server.
Option	Description									
enable	Enable synchronization with NTP Server.									
disable	Disable synchronization with NTP Server.									
server-mode	Enable/disable FortiGate NTP Server Mode. Your FortiGate becomes an NTP server for other devices on your network. The FortiGate relays NTP requests to its configured NTP server.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable FortiGate NTP Server Mode.</td></tr><tr><td>disable</td><td>Disable FortiGate NTP Server Mode.</td></tr></table>				Option	Description	enable	Enable FortiGate NTP Server Mode.	disable	Disable FortiGate NTP Server Mode.
Option	Description									
enable	Enable FortiGate NTP Server Mode.									
disable	Disable FortiGate NTP Server Mode.									
source-ip	Source IP address for communication to the NTP server.	ipv4-address	Not Specified	0.0.0.0						
source-ip6	Source IPv6 address for communication to the NTP server.	ipv6-address	Not Specified	::						
syncinterval	NTP synchronization interval.	integer	Minimum value: 1 Maximum value: 1440	60						



Parameter	Description	Type	Size	Default						
type	Use the FortiGuard NTP server or any other available NTP Server.	option	-	fortiguard						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>fortiguard</i></td><td>Use the FortiGuard NTP server.</td></tr><tr><td><i>custom</i></td><td>Use any other available NTP server.</td></tr></table>				Option	Description	<i>fortiguard</i>	Use the FortiGuard NTP server.	<i>custom</i>	Use any other available NTP server.
Option	Description									
<i>fortiguard</i>	Use the FortiGuard NTP server.									
<i>custom</i>	Use any other available NTP server.									

## config ntpserver

Parameter	Description	Type	Size	Default						
id	NTP server ID.	integer	Minimum value: 0 Maximum value: 4294967295	0						
server	IP address or hostname of the NTP Server.	string	Maximum length: 63							
ntp3	Enable to use NTPv3 instead of NTPv4.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable NTPv3.</td></tr><tr><td>disable</td><td>Disable NTPv3 (use NTPv4).</td></tr></table>				Option	Description	enable	Enable NTPv3.	disable	Disable NTPv3 (use NTPv4).
Option	Description									
enable	Enable NTPv3.									
disable	Disable NTPv3 (use NTPv4).									
authentication	Enable/disable MD5(NTPv3)/SHA1(NTPv4) authentication.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable MD5(NTPv3)/SHA1(NTPv4) authentication.</td></tr><tr><td>disable</td><td>Disable MD5(NTPv3)/SHA1(NTPv4) authentication.</td></tr></table>				Option	Description	enable	Enable MD5(NTPv3)/SHA1(NTPv4) authentication.	disable	Disable MD5(NTPv3)/SHA1(NTPv4) authentication.
Option	Description									
enable	Enable MD5(NTPv3)/SHA1(NTPv4) authentication.									
disable	Disable MD5(NTPv3)/SHA1(NTPv4) authentication.									
key	Key for MD5(NTPv3)/SHA1(NTPv4) authentication.	password	Not Specified							
key-id	Key ID for authentication.	integer	Minimum value: 0 Maximum value: 4294967295	0						
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto						

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>auto</i>	Set outgoing interface automatically.		
	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.		
	<i>specify</i>	Set outgoing interface manually.		
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	

## config system object-tagging

Configure object tagging.

```

config system object-tagging
    Description: Configure object tagging.
    edit <category>
        set address [disable|mandatory|...]
        set color {integer}
        set device [disable|mandatory|...]
        set interface [disable|mandatory|...]
        set multiple [enable|disable]
        set tags <name1>, <name2>, ...
    next
end

```

## config system object-tagging

Parameter	Description	Type	Size	Default
address	Address.	option	-	optional
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable.		
	<i>mandatory</i>	Mandatory.		
	<i>optional</i>	Optional.		
category	Tag Category.	string	Maximum length: 63	
color	Color of icon on the GUI.	integer	Minimum value: 0 Maximum value: 32	0
device	Device.	option	-	optional

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable.		
	<i>mandatory</i>	Mandatory.		
	<i>optional</i>	Optional.		
interface	Interface.	option	-	optional
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable.		
	<i>mandatory</i>	Mandatory.		
	<i>optional</i>	Optional.		
multiple	Allow multiple tag selection.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable multi-tagging.		
	<i>disable</i>	Disable multi-tagging.		
tags <name>	Tags. Tag name.	string	Maximum length: 79	

## config system password-policy-guest-admin

Configure the password policy for guest administrators.

```

config system password-policy-guest-admin
    Description: Configure the password policy for guest administrators.
    set apply-to {option1}, {option2}, ...
    set expire-day {integer}
    set expire-status [enable|disable]
    set min-change-characters {integer}
    set min-lower-case-letter {integer}
    set min-non-alphanumeric {integer}
    set min-number {integer}
    set min-upper-case-letter {integer}
    set minimum-length {integer}
    set reuse-password [enable|disable]
    set status [enable|disable]
end

```

## config system password-policy-guest-admin

Parameter	Description	Type	Size	Default						
apply-to	Guest administrator to which this password policy applies.	option	-	guest-admin-password						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>guest-admin-password</i></td><td>Apply to guest administrator password.</td></tr></table>	Option	Description	<i>guest-admin-password</i>	Apply to guest administrator password.					
Option	Description									
<i>guest-admin-password</i>	Apply to guest administrator password.									
expire-day	Number of days after which passwords expire.	integer	Minimum value: 1 Maximum value: 999	90						
expire-status	Enable/disable password expiration.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Passwords expire after expire-day days.</td></tr><tr><td><i>disable</i></td><td>Passwords do not expire.</td></tr></table>	Option	Description	<i>enable</i>	Passwords expire after expire-day days.	<i>disable</i>	Passwords do not expire.			
Option	Description									
<i>enable</i>	Passwords expire after expire-day days.									
<i>disable</i>	Passwords do not expire.									
min-change-characters	Minimum number of unique characters in new password which do not exist in old password.	integer	Minimum value: 0 Maximum value: 128	0						
min-lower-case-letter	Minimum number of lowercase characters in password.	integer	Minimum value: 0 Maximum value: 128	0						
min-non-alphanumeric	Minimum number of non-alphanumeric characters in password.	integer	Minimum value: 0 Maximum value: 128	0						
min-number	Minimum number of numeric characters in password.	integer	Minimum value: 0 Maximum value: 128	0						
min-upper-case-letter	Minimum number of uppercase characters in password.	integer	Minimum value: 0 Maximum value: 128	0						

Parameter	Description	Type	Size	Default						
minimum-length	Minimum password length.	integer	Minimum value: 8 Maximum value: 128	8						
reuse-password	Enable/disable reuse of password. If both reuse-password and min-change-characters are enabled, min-change-characters overrides.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Administrators are allowed to reuse the same password.</td></tr><tr><td><i>disable</i></td><td>Administrators must create a new password.</td></tr></table>				Option	Description	<i>enable</i>	Administrators are allowed to reuse the same password.	<i>disable</i>	Administrators must create a new password.
Option	Description									
<i>enable</i>	Administrators are allowed to reuse the same password.									
<i>disable</i>	Administrators must create a new password.									
status	Enable/disable setting a password policy for locally defined administrator passwords and IPsec VPN pre-shared keys.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable password policy.</td></tr><tr><td><i>disable</i></td><td>Disable password policy.</td></tr></table>				Option	Description	<i>enable</i>	Enable password policy.	<i>disable</i>	Disable password policy.
Option	Description									
<i>enable</i>	Enable password policy.									
<i>disable</i>	Disable password policy.									

## config system password-policy

Configure password policy for locally defined administrator passwords and IPsec VPN pre-shared keys.

```

config system password-policy
    Description: Configure password policy for locally defined administrator passwords and
IPsec VPN pre-shared keys.
    set apply-to {option1}, {option2}, ...
    set expire-day {integer}
    set expire-status [enable|disable]
    set min-change-characters {integer}
    set min-lower-case-letter {integer}
    set min-non-alphanumeric {integer}
    set min-number {integer}
    set min-upper-case-letter {integer}
    set minimum-length {integer}
    set reuse-password [enable|disable]
    set status [enable|disable]
end

```

## config system password-policy

Parameter	Description	Type	Size	Default						
apply-to	Apply password policy to administrator passwords or IPsec pre-shared keys or both. Separate entries with a space.	option	-	admin-password						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>admin-password</i></td><td>Apply to administrator passwords.</td></tr><tr><td><i>ipsec-preshared-key</i></td><td>Apply to IPsec pre-shared keys.</td></tr></table>	Option	Description	<i>admin-password</i>	Apply to administrator passwords.	<i>ipsec-preshared-key</i>	Apply to IPsec pre-shared keys.			
Option	Description									
<i>admin-password</i>	Apply to administrator passwords.									
<i>ipsec-preshared-key</i>	Apply to IPsec pre-shared keys.									
expire-day	Number of days after which passwords expire.	integer	Minimum value: 1 Maximum value: 999	90						
expire-status	Enable/disable password expiration.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Passwords expire after expire-day days.</td></tr><tr><td><i>disable</i></td><td>Passwords do not expire.</td></tr></table>	Option	Description	<i>enable</i>	Passwords expire after expire-day days.	<i>disable</i>	Passwords do not expire.			
Option	Description									
<i>enable</i>	Passwords expire after expire-day days.									
<i>disable</i>	Passwords do not expire.									
min-change-characters	Minimum number of unique characters in new password which do not exist in old password.	integer	Minimum value: 0 Maximum value: 128	0						
min-lower-case-letter	Minimum number of lowercase characters in password.	integer	Minimum value: 0 Maximum value: 128	0						
min-non-alphanumeric	Minimum number of non-alphanumeric characters in password.	integer	Minimum value: 0 Maximum value: 128	0						
min-number	Minimum number of numeric characters in password.	integer	Minimum value: 0 Maximum value: 128	0						
min-upper-case-letter	Minimum number of uppercase characters in password.	integer	Minimum value: 0 Maximum value: 128	0						

Parameter	Description	Type	Size	Default						
minimum-length	Minimum password length.	integer	Minimum value: 8 Maximum value: 128	8						
reuse-password	Enable/disable reuse of password. If both reuse-password and min-change-characters are enabled, min-change-characters overrides.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Administrators are allowed to reuse the same password.</td></tr><tr><td><i>disable</i></td><td>Administrators must create a new password.</td></tr></table>				Option	Description	<i>enable</i>	Administrators are allowed to reuse the same password.	<i>disable</i>	Administrators must create a new password.
Option	Description									
<i>enable</i>	Administrators are allowed to reuse the same password.									
<i>disable</i>	Administrators must create a new password.									
status	Enable/disable setting a password policy for locally defined administrator passwords and IPsec VPN pre-shared keys.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable password policy.</td></tr><tr><td><i>disable</i></td><td>Disable password policy.</td></tr></table>				Option	Description	<i>enable</i>	Enable password policy.	<i>disable</i>	Disable password policy.
Option	Description									
<i>enable</i>	Enable password policy.									
<i>disable</i>	Disable password policy.									

## config system physical-switch



This command is available for model(s): FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 140E-POE, FortiGate 140E, FortiGate 1800F, FortiGate 1801F, FortiGate 200F, FortiGate 201F, FortiGate 2600F, FortiGate 2601F, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3500F, FortiGate 3501F, FortiGate 3800D, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 600F, FortiGate 601F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 90E, FortiGate 91E, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 1000D, FortiGate 1200D, FortiGate 1500DT, FortiGate 1500D, FortiGate 2000E, FortiGate 200E, FortiGate 201E, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 3000D, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 601E, FortiGate 800D, FortiGate 900D, FortiGate VM64.

Configure physical switches.

```
config system physical-switch
  Description: Configure physical switches.
  edit <name>
    set age-enable [enable|disable]
    set age-val {integer}
  next
end
```

## config system physical-switch

Parameter	Description	Type	Size	Default
age-enable	Enable/disable layer 2 age timer.	option	-	disable
	<b>Option</b>			
	<i>enable</i>			
	<i>disable</i>			
age-val	Layer 2 table age timer value.	integer	Minimum value: 0 Maximum value: 4294967295	3158067
name	Name.	string	Maximum length: 15	

## config system pppoe-interface

Configure the PPPoE interfaces.

```
config system pppoe-interface
  Description: Configure the PPPoE interfaces.
  edit <name>
    set ac-name {string}
    set auth-type [auto|pap|...]
    set device {string}
    set dial-on-demand [enable|disable]
    set disc-retry-timeout {integer}
    set idle-timeout {integer}
    set ipunnumbered {ipv4-address}
    set ipv6 [enable|disable]
    set lcp-echo-interval {integer}
    set lcp-max-echo-fails {integer}
    set padt-retry-timeout {integer}
    set password {password}
    set pppoe-unnumbered-negotiate [enable|disable]
    set service-name {string}
    set username {string}
```



```
next
end
```

## config system pppoe-interface

Parameter	Description	Type	Size	Default												
ac-name	PPPoE AC name.	string	Maximum length: 63													
auth-type	PPP authentication type to use.	option	-	auto												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto</i></td><td>Automatically choose the authentication method.</td></tr><tr><td><i>pap</i></td><td>PAP authentication.</td></tr><tr><td><i>chap</i></td><td>CHAP authentication.</td></tr><tr><td><i>mschapv1</i></td><td>MS-CHAPv1 authentication.</td></tr><tr><td><i>mschapv2</i></td><td>MS-CHAPv2 authentication.</td></tr></table>				Option	Description	<i>auto</i>	Automatically choose the authentication method.	<i>pap</i>	PAP authentication.	<i>chap</i>	CHAP authentication.	<i>mschapv1</i>	MS-CHAPv1 authentication.	<i>mschapv2</i>	MS-CHAPv2 authentication.
	Option	Description														
	<i>auto</i>	Automatically choose the authentication method.														
	<i>pap</i>	PAP authentication.														
	<i>chap</i>	CHAP authentication.														
	<i>mschapv1</i>	MS-CHAPv1 authentication.														
<i>mschapv2</i>	MS-CHAPv2 authentication.															
device	Name for the physical interface.	string	Maximum length: 15													
dial-on-demand	Enable/disable dial on demand to dial the PPPoE interface when packets are routed to the PPPoE interface.	option	-	disable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable dial on demand.</td></tr><tr><td><i>disable</i></td><td>Disable dial on demand.</td></tr></table>				Option	Description	<i>enable</i>	Enable dial on demand.	<i>disable</i>	Disable dial on demand.						
	Option	Description														
	<i>enable</i>	Enable dial on demand.														
<i>disable</i>	Disable dial on demand.															
disc-retry-timeout	PPPoE discovery init timeout value in.	integer	Minimum value: 0 Maximum value: 4294967295	1												
idle-timeout	PPPoE auto disconnect after idle timeout.	integer	Minimum value: 0 Maximum value: 4294967295	0												
ipunnumbered	PPPoE unnumbered IP.	ipv4-address	Not Specified	0.0.0.0												
ipv6	Enable/disable IPv6 Control Protocol (IPv6CP).	option	-	disable												

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable IPv6CP.		
	<i>disable</i>	Disable IPv6CP.		
lcp-echo-interval	Time in seconds between PPPoE Link Control Protocol (LCP) echo requests.	integer	Minimum value: 0 Maximum value: 32767	5
lcp-max-echo-fails	Maximum missed LCP echo messages before disconnect.	integer	Minimum value: 0 Maximum value: 32767	3
name	Name of the PPPoE interface.	string	Maximum length: 15	
padt-retry-timeout	PPPoE terminate timeout value in.	integer	Minimum value: 0 Maximum value: 4294967295	1
password	Enter the password.	password	Not Specified	
pppoe-unnumbered-negotiate	Enable/disable PPPoE unnumbered negotiation.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable PPPoE unnumbered negotiation.		
	<i>disable</i>	Disable PPPoE unnumbered negotiation.		
service-name	PPPoE service name.	string	Maximum length: 63	
username	User name.	string	Maximum length: 64	

## config system probe-response

Configure system probe response.

```
config system probe-response
  Description: Configure system probe response.
  set http-probe-value {string}
  set mode [none|http-probe|...]
  set password {password}
```

```

set port {integer}
set security-mode [none|authentication]
set timeout {integer}
set ttl-mode [reinit|decrease|...]
end

```

## config system probe-response

Parameter	Description	Type	Size	Default
http-probe-value	Value to respond to the monitoring server.	string	Maximum length: 1024	OK
mode	SLA response mode.	option	-	none
	<div><div>Option</div><div>Description</div></div>			
	<i>none</i>	Disable probe.		
	<i>http-probe</i>	HTTP probe.		
	<i>twamp</i>	Two way active measurement protocol.		
password	TWAMP responder password in authentication mode.	password	Not Specified	
port	Port number to response.	integer	Minimum value: 1 Maximum value: 65535	8008
security-mode	TWAMP responder security mode.	option	-	none
	<div><div>Option</div><div>Description</div></div>			
	<i>none</i>	Unauthenticated mode.		
	<i>authentication</i>	Authenticated mode.		
timeout	An inactivity timer for a twamp test session.	integer	Minimum value: 10 Maximum value: 3600	300
ttl-mode	Mode for TWAMP packet TTL modification.	option	-	retain
	<div><div>Option</div><div>Description</div></div>			
	<i>reinit</i>	Reinitialize TTL.		
	<i>decrease</i>	Decrease TTL.		
	<i>retain</i>	Retain TTL.		

## config system proxy-arp

Configure proxy-ARP.

```
config system proxy-arp
  Description: Configure proxy-ARP.
  edit <id>
    set end-ip {ipv4-address}
    set interface {string}
    set ip {ipv4-address}
  next
end
```

## config system proxy-arp

Parameter	Description	Type	Size	Default
end-ip	End IP of IP range to be proxied.	ipv4-address	Not Specified	0.0.0.0
id	Unique integer ID of the entry.	integer	Minimum value: 0 Maximum value: 4294967295	0
interface	Interface acting proxy-ARP.	string	Maximum length: 15	
ip	IP address or start IP to be proxied.	ipv4-address	Not Specified	0.0.0.0

## config system ptp

Configure system PTP information.

```
config system ptp
  Description: Configure system PTP information.
  set delay-mechanism [E2E|P2P]
  set interface {string}
  set mode [multicast|hybrid]
  set request-interval {integer}
  config server-interface
    Description: FortiGate interface(s) with PTP server mode enabled. Devices on your
network can contact these interfaces for PTP services.
    edit <id>
      set server-interface-name {string}
      set delay-mechanism [E2E|P2P]
    next
  end
  set server-mode [enable|disable]
  set status [enable|disable]
end
```

## config system ptp

Parameter	Description	Type	Size	Default						
delay-mechanism	End to end delay detection or peer to peer delay detection.	option	-	E2E						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>E2E</i></td><td>End to end delay detection.</td></tr><tr><td><i>P2P</i></td><td>Peer to peer delay detection.</td></tr></table>	Option	Description	<i>E2E</i>	End to end delay detection.	<i>P2P</i>	Peer to peer delay detection.			
Option	Description									
<i>E2E</i>	End to end delay detection.									
<i>P2P</i>	Peer to peer delay detection.									
interface	PTP client will reply through this interface.	string	Maximum length: 15							
mode	Multicast transmission or hybrid transmission.	option	-	multicast						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>multicast</i></td><td>Send PTP packets with multicast.</td></tr><tr><td><i>hybrid</i></td><td>Send PTP packets with unicast and multicast.</td></tr></table>	Option	Description	<i>multicast</i>	Send PTP packets with multicast.	<i>hybrid</i>	Send PTP packets with unicast and multicast.			
Option	Description									
<i>multicast</i>	Send PTP packets with multicast.									
<i>hybrid</i>	Send PTP packets with unicast and multicast.									
request-interval	The delay request value is the logarithmic mean interval in seconds between the delay request messages sent by the slave to the master.	integer	Minimum value: 1 Maximum value: 6	1						
server-mode	Enable/disable FortiGate PTP server mode. Your FortiGate becomes an PTP server for other devices on your network.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable FortiGate PTP server mode.</td></tr><tr><td><i>disable</i></td><td>Disable FortiGate PTP server mode.</td></tr></table>	Option	Description	<i>enable</i>	Enable FortiGate PTP server mode.	<i>disable</i>	Disable FortiGate PTP server mode.			
Option	Description									
<i>enable</i>	Enable FortiGate PTP server mode.									
<i>disable</i>	Disable FortiGate PTP server mode.									
status	Enable/disable setting the FortiGate system time by synchronizing with an PTP Server.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable synchronization with PTP Server.</td></tr><tr><td><i>disable</i></td><td>Disable synchronization with PTP Server.</td></tr></table>	Option	Description	<i>enable</i>	Enable synchronization with PTP Server.	<i>disable</i>	Disable synchronization with PTP Server.			
Option	Description									
<i>enable</i>	Enable synchronization with PTP Server.									
<i>disable</i>	Disable synchronization with PTP Server.									

## config server-interface

Parameter	Description	Type	Size	Default						
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0						
server-interface-name	Interface name.	string	Maximum length: 15							
delay-mechanism	End to end delay detection or peer to peer delay detection.	option	-	E2E						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>E2E</td><td>End to end delay detection.</td></tr><tr><td>P2P</td><td>Peer to peer delay detection.</td></tr></table>				Option	Description	E2E	End to end delay detection.	P2P	Peer to peer delay detection.
	Option	Description								
	E2E	End to end delay detection.								
P2P	Peer to peer delay detection.									

## config system replacemsg-group

Configure replacement message groups.

```
config system replacemsg-group
  Description: Configure replacement message groups.
  edit <name>
    config admin
      Description: Replacement message table entries.
      edit <msg-type>
        set buffer {var-string}
        set header [none|http|...]
        set format [none|text|...]
      next
    end
    config alertmail
      Description: Replacement message table entries.
      edit <msg-type>
        set buffer {var-string}
        set header [none|http|...]
        set format [none|text|...]
      next
    end
    config auth
      Description: Replacement message table entries.
      edit <msg-type>
        set buffer {var-string}
        set header [none|http|...]
        set format [none|text|...]
      next
    end
  end
```

```

config automation
    Description: Replacement message table entries.
    edit <msg-type>
        set buffer {var-string}
        set header [none|http|...]
        set format [none|text|...]
    next
end
set comment {var-string}
config custom-message
    Description: Replacement message table entries.
    edit <msg-type>
        set buffer {var-string}
        set header [none|http|...]
        set format [none|text|...]
    next
end
config fortiguard-wf
    Description: Replacement message table entries.
    edit <msg-type>
        set buffer {var-string}
        set header [none|http|...]
        set format [none|text|...]
    next
end
config ftp
    Description: Replacement message table entries.
    edit <msg-type>
        set buffer {var-string}
        set header [none|http|...]
        set format [none|text|...]
    next
end
set group-type [default|utm|...]
config http
    Description: Replacement message table entries.
    edit <msg-type>
        set buffer {var-string}
        set header [none|http|...]
        set format [none|text|...]
    next
end
config icap
    Description: Replacement message table entries.
    edit <msg-type>
        set buffer {var-string}
        set header [none|http|...]
        set format [none|text|...]
    next
end
config mail
    Description: Replacement message table entries.
    edit <msg-type>
        set buffer {var-string}
        set header [none|http|...]
        set format [none|text|...]

```

```
        next
    end
    config nac-quar
        Description: Replacement message table entries.
        edit <msg-type>
            set buffer {var-string}
            set header [none|http|...]
            set format [none|text|...]
        next
    end
    config spam
        Description: Replacement message table entries.
        edit <msg-type>
            set buffer {var-string}
            set header [none|http|...]
            set format [none|text|...]
        next
    end
    config sslvpn
        Description: Replacement message table entries.
        edit <msg-type>
            set buffer {var-string}
            set header [none|http|...]
            set format [none|text|...]
        next
    end
    config traffic-quota
        Description: Replacement message table entries.
        edit <msg-type>
            set buffer {var-string}
            set header [none|http|...]
            set format [none|text|...]
        next
    end
    config utm
        Description: Replacement message table entries.
        edit <msg-type>
            set buffer {var-string}
            set header [none|http|...]
            set format [none|text|...]
        next
    end
    config webproxy
        Description: Replacement message table entries.
        edit <msg-type>
            set buffer {var-string}
            set header [none|http|...]
            set format [none|text|...]
        next
    end
next
end
```



## config system replacemsg-group

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 255	
group-type	Group type.	option	-	default
	<b>Option</b>	<b>Description</b>		
	<i>default</i>	Per-vdom replacement messages.		
	<i>utm</i>	For use with UTM settings in firewall policies.		
	<i>auth</i>	For use with authentication pages in firewall policies.		
name	Group name.	string	Maximum length: 35	

## config admin

Parameter	Description	Type	Size	Default
msg-type	Message type.	string	Maximum length: 28	
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	none
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	No header type.		
	<i>http</i>	HTTP		
	<i>8bit</i>	8 bit.		
format	Format flag.	option	-	none
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	No format type.		
	<i>text</i>	Text format.		
	<i>html</i>	HTML format.		

## config alertmail

Parameter	Description	Type	Size	Default
msg-type	Message type.	string	Maximum length: 28	
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	none
	OptionDescription			
	none	No header type.		
	http	HTTP		
	8bit	8 bit.		
format	Format flag.	option	-	none
	OptionDescription			
	none	No format type.		
	text	Text format.		
	html	HTML format.		

## config auth

Parameter	Description	Type	Size	Default								
msg-type	Message type.	string	Maximum length: 28									
buffer	Message string.	var-string	Maximum length: 32768									
header	Header flag.	option	-	none								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>No header type.</td></tr><tr><td><i>http</i></td><td>HTTP</td></tr><tr><td><i>8bit</i></td><td>8 bit.</td></tr></table>				Option	Description	<i>none</i>	No header type.	<i>http</i>	HTTP	<i>8bit</i>	8 bit.
	Option	Description										
	<i>none</i>	No header type.										
	<i>http</i>	HTTP										
<i>8bit</i>	8 bit.											
format	Format flag.	option	-	none								

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	No format type.		
	<i>text</i>	Text format.		
	<i>html</i>	HTML format.		

### config automation

Parameter	Description	Type	Size	Default
msg-type	Message type.	string	Maximum length: 28	
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	none
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	No header type.		
	<i>http</i>	HTTP		
	<i>8bit</i>	8 bit.		
format	Format flag.	option	-	none
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	No format type.		
	<i>text</i>	Text format.		
	<i>html</i>	HTML format.		

### config custom-message

Parameter	Description	Type	Size	Default
msg-type	Message type.	string	Maximum length: 28	
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	none

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	No header type.		
	<i>http</i>	HTTP		
	<i>8bit</i>	8 bit.		
format	Format flag.	option	-	none
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	No format type.		
	<i>text</i>	Text format.		
	<i>html</i>	HTML format.		

### config fortiguard-wf

Parameter	Description	Type	Size	Default
msg-type	Message type.	string	Maximum length: 28	
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	none
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	No header type.		
	<i>http</i>	HTTP		
	<i>8bit</i>	8 bit.		
format	Format flag.	option	-	none
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	No format type.		
	<i>text</i>	Text format.		
	<i>html</i>	HTML format.		

## config ftp

Parameter	Description	Type	Size	Default
msg-type	Message type.	string	Maximum length: 28	
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	none
	OptionDescription			
	none	No header type.		
	http	HTTP		
	8bit	8 bit.		
format	Format flag.	option	-	none
	OptionDescription			
	none	No format type.		
	text	Text format.		
	html	HTML format.		

## config http

Parameter	Description	Type	Size	Default								
msg-type	Message type.	string	Maximum length: 28									
buffer	Message string.	var-string	Maximum length: 32768									
header	Header flag.	option	-	none								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>No header type.</td></tr><tr><td><i>http</i></td><td>HTTP</td></tr><tr><td><i>8bit</i></td><td>8 bit.</td></tr></table>				Option	Description	<i>none</i>	No header type.	<i>http</i>	HTTP	<i>8bit</i>	8 bit.
	Option	Description										
	<i>none</i>	No header type.										
	<i>http</i>	HTTP										
<i>8bit</i>	8 bit.											
format	Format flag.	option	-	none								

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	No format type.		
	<i>text</i>	Text format.		
	<i>html</i>	HTML format.		

### config icap

Parameter	Description	Type	Size	Default
msg-type	Message type.	string	Maximum length: 28	
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	none
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	No header type.		
	<i>http</i>	HTTP		
	<i>8bit</i>	8 bit.		
format	Format flag.	option	-	none
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	No format type.		
	<i>text</i>	Text format.		
	<i>html</i>	HTML format.		

### config mail

Parameter	Description	Type	Size	Default
msg-type	Message type.	string	Maximum length: 28	
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	none

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	No header type.		
	<i>http</i>	HTTP		
	<i>8bit</i>	8 bit.		
format	Format flag.	option	-	none
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	No format type.		
	<i>text</i>	Text format.		
	<i>html</i>	HTML format.		

### config nac-quar

Parameter	Description	Type	Size	Default
msg-type	Message type.	string	Maximum length: 28	
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	none
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	No header type.		
	<i>http</i>	HTTP		
	<i>8bit</i>	8 bit.		
format	Format flag.	option	-	none
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	No format type.		
	<i>text</i>	Text format.		
	<i>html</i>	HTML format.		

## config spam

Parameter	Description	Type	Size	Default
msg-type	Message type.	string	Maximum length: 28	
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	none
	OptionDescription			
	none	No header type.		
	http	HTTP		
	8bit	8 bit.		
format	Format flag.	option	-	none
	OptionDescription			
	none	No format type.		
	text	Text format.		
	html	HTML format.		

## config sslvpn

Parameter	Description	Type	Size	Default								
msg-type	Message type.	string	Maximum length: 28									
buffer	Message string.	var-string	Maximum length: 32768									
header	Header flag.	option	-	none								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>No header type.</td></tr><tr><td><i>http</i></td><td>HTTP</td></tr><tr><td><i>8bit</i></td><td>8 bit.</td></tr></table>				Option	Description	<i>none</i>	No header type.	<i>http</i>	HTTP	<i>8bit</i>	8 bit.
	Option	Description										
	<i>none</i>	No header type.										
	<i>http</i>	HTTP										
<i>8bit</i>	8 bit.											
format	Format flag.	option	-	none								



Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	No format type.		
	<i>text</i>	Text format.		
	<i>html</i>	HTML format.		

### config traffic-quota

Parameter	Description	Type	Size	Default
msg-type	Message type.	string	Maximum length: 28	
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	none
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	No header type.		
	<i>http</i>	HTTP		
	<i>8bit</i>	8 bit.		
format	Format flag.	option	-	none
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	No format type.		
	<i>text</i>	Text format.		
	<i>html</i>	HTML format.		

### config utm

Parameter	Description	Type	Size	Default
msg-type	Message type.	string	Maximum length: 28	
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	none

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	No header type.		
	<i>http</i>	HTTP		
	<i>8bit</i>	8 bit.		
format	Format flag.	option	-	none
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	No format type.		
	<i>text</i>	Text format.		
	<i>html</i>	HTML format.		

### config webproxy

Parameter	Description	Type	Size	Default
msg-type	Message type.	string	Maximum length: 28	
buffer	Message string.	var-string	Maximum length: 32768	
header	Header flag.	option	-	none
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	No header type.		
	<i>http</i>	HTTP		
	<i>8bit</i>	8 bit.		
format	Format flag.	option	-	none
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	No format type.		
	<i>text</i>	Text format.		
	<i>html</i>	HTML format.		

### config system replacemsg-image

Configure replacement message images.

```

config system replacemsg-image
  Description: Configure replacement message images.
  edit <name>
    set image-base64 {var-string}
    set image-type [gif|jpg|...]
  next
end

```

## config system replacemsg-image

Parameter	Description	Type	Size	Default
image-base64	Image data.	var-string	Maximum length: 32768	
image-type	Image type.	option	-	png
	Option	Description		
	gif	GIF image.		
	jpg	JPEG image.		
	tiff	TIFF image.		
	png	PNG image.		
name	Image name.	string	Maximum length: 23	

## config system replacemsg admin

Replacement messages.

```

config system replacemsg admin
  Description: Replacement messages.
  edit <msg-type>
    set buffer {var-string}
    set format [none|text|...]
    set header [none|http|...]
  next
end

```

## config system replacemsg admin

Parameter	Description	Type	Size	Default
buffer	Message string.	var-string	Maximum length: 32768	

Parameter	Description	Type	Size	Default
format	Format flag.	option	-	
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	No format type.		
	<i>text</i>	Text format.		
	<i>html</i>	HTML format.		
header	Header flag.	option	-	
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	No header type.		
	<i>http</i>	HTTP		
	<i>8bit</i>	8 bit.		
msg-type	Message type.	string	Maximum length: 28	

## config system replacemsg alertmail

Replacement messages.

```
config system replacemsg alertmail
  Description: Replacement messages.
  edit <msg-type>
    set buffer {var-string}
    set format [none|text|...]
    set header [none|http|...]
  next
end
```

## config system replacemsg alertmail

Parameter	Description	Type	Size	Default
buffer	Message string.	var-string	Maximum length: 32768	
format	Format flag.	option	-	
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	No format type.		

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>text</i>	Text format.		
	<i>html</i>	HTML format.		
header	Header flag.	option	-	
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	No header type.		
	<i>http</i>	HTTP		
	<i>8bit</i>	8 bit.		
msg-type	Message type.	string	Maximum length: 28	

## config system replacemsg auth

Replacement messages.

```
config system replacemsg auth
    Description: Replacement messages.
    edit <msg-type>
        set buffer {var-string}
        set format [none|text|...]
        set header [none|http|...]
    next
end
```

## config system replacemsg auth

Parameter	Description	Type	Size	Default
buffer	Message string.	var-string	Maximum length: 32768	
format	Format flag.	option	-	
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	No format type.		
	<i>text</i>	Text format.		
	<i>html</i>	HTML format.		
header	Header flag.	option	-	

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	No header type.		
	<i>http</i>	HTTP		
	<i>8bit</i>	8 bit.		
msg-type	Message type.	string	Maximum length: 28	

## config system replacemsg automation

Replacement messages.

```

config system replacemsg automation
    Description: Replacement messages.
    edit <msg-type>
        set buffer {var-string}
        set format [none|text|...]
        set header [none|http|...]
    next
end

```

## config system replacemsg automation

Parameter	Description	Type	Size	Default
buffer	Message string.	var-string	Maximum length: 32768	
format	Format flag.	option	-	
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	No format type.		
	<i>text</i>	Text format.		
	<i>html</i>	HTML format.		
header	Header flag.	option	-	
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	No header type.		
	<i>http</i>	HTTP		
	<i>8bit</i>	8 bit.		

Parameter	Description	Type	Size	Default
msg-type	Message type.	string	Maximum length: 28	

## config system replacemsg custom-message

Replacement messages.

```
config system replacemsg custom-message
    Description: Replacement messages.
    edit <msg-type>
        set buffer {var-string}
        set format [none|text|...]
        set header [none|http|...]
    next
end
```

## config system replacemsg custom-message

Parameter	Description	Type	Size	Default
buffer	Message string.	var-string	Maximum length: 32768	
format	Format flag.	option	-	
	OptionDescription			
	none	No format type.		
	text	Text format.		
	html	HTML format.		
header	Header flag.	option	-	
	OptionDescription			
	none	No header type.		
	http	HTTP		
	8bit	8 bit.		
msg-type	Message type.	string	Maximum length: 28	

## config system replacemsg fortiguard-wf

Replacement messages.

```

config system replacemsg fortiguard-wf
  Description: Replacement messages.
  edit <msg-type>
    set buffer {var-string}
    set format [none|text|...]
    set header [none|http|...]
  next
end

```

## config system replacemsg fortiguard-wf

Parameter	Description	Type	Size	Default
buffer	Message string.	var-string	Maximum length: 32768	
format	Format flag.	option	-	
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	No format type.		
	<i>text</i>	Text format.		
	<i>html</i>	HTML format.		
header	Header flag.	option	-	
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	No header type.		
	<i>http</i>	HTTP		
	<i>8bit</i>	8 bit.		
msg-type	Message type.	string	Maximum length: 28	

## config system replacemsg ftp

Replacement messages.

```

config system replacemsg ftp
  Description: Replacement messages.
  edit <msg-type>
    set buffer {var-string}
    set format [none|text|...]
    set header [none|http|...]
  next
end

```



## config system replacemsg ftp

Parameter	Description	Type	Size	Default								
buffer	Message string.	var-string	Maximum length: 32768									
format	Format flag.	option	-									
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>No format type.</td></tr><tr><td><i>text</i></td><td>Text format.</td></tr><tr><td><i>html</i></td><td>HTML format.</td></tr></table>				Option	Description	<i>none</i>	No format type.	<i>text</i>	Text format.	<i>html</i>	HTML format.
	Option	Description										
	<i>none</i>	No format type.										
	<i>text</i>	Text format.										
<i>html</i>	HTML format.											
header	Header flag.	option	-									
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>No header type.</td></tr><tr><td><i>http</i></td><td>HTTP</td></tr><tr><td><i>8bit</i></td><td>8 bit.</td></tr></table>				Option	Description	<i>none</i>	No header type.	<i>http</i>	HTTP	<i>8bit</i>	8 bit.
	Option	Description										
	<i>none</i>	No header type.										
	<i>http</i>	HTTP										
<i>8bit</i>	8 bit.											
msg-type	Message type.	string	Maximum length: 28									

## config system replacemsg http

Replacement messages.

```
config system replacemsg http
  Description: Replacement messages.
  edit <msg-type>
    set buffer {var-string}
    set format [none|text|...]
    set header [none|http|...]
  next
end
```

## config system replacemsg http

Parameter	Description	Type	Size	Default
buffer	Message string.	var-string	Maximum length: 32768	

Parameter	Description	Type	Size	Default
format	Format flag.	option	-	
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	No format type.		
	<i>text</i>	Text format.		
	<i>html</i>	HTML format.		
header	Header flag.	option	-	
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	No header type.		
	<i>http</i>	HTTP		
	<i>8bit</i>	8 bit.		
msg-type	Message type.	string	Maximum length: 28	

## config system replacemsg icap

Replacement messages.

```
config system replacemsg icap
    Description: Replacement messages.
    edit <msg-type>
        set buffer {var-string}
        set format [none|text|...]
        set header [none|http|...]
    next
end
```

## config system replacemsg icap

Parameter	Description	Type	Size	Default
buffer	Message string.	var-string	Maximum length: 32768	
format	Format flag.	option	-	
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	No format type.		

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>text</i></td><td>Text format.</td></tr><tr><td><i>html</i></td><td>HTML format.</td></tr></table>	Option	Description	<i>text</i>	Text format.	<i>html</i>	HTML format.					
	Option	Description										
	<i>text</i>	Text format.										
<i>html</i>	HTML format.											
header	Header flag.	option	-									
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>No header type.</td></tr><tr><td><i>http</i></td><td>HTTP</td></tr><tr><td><i>8bit</i></td><td>8 bit.</td></tr></table>	Option	Description	<i>none</i>	No header type.	<i>http</i>	HTTP	<i>8bit</i>	8 bit.			
	Option	Description										
	<i>none</i>	No header type.										
	<i>http</i>	HTTP										
<i>8bit</i>	8 bit.											
msg-type	Message type.	string	Maximum length: 28									

## config system replacemsg mail

Replacement messages.

```

config system replacemsg mail
    Description: Replacement messages.
    edit <msg-type>
        set buffer {var-string}
        set format [none|text|...]
        set header [none|http|...]
    next
end

```

## config system replacemsg mail

Parameter	Description	Type	Size	Default
buffer	Message string.	var-string	Maximum length: 32768	
format	Format flag.	option	-	
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	No format type.		
	<i>text</i>	Text format.		
	<i>html</i>	HTML format.		
header	Header flag.	option	-	

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	No header type.		
	<i>http</i>	HTTP		
	<i>8bit</i>	8 bit.		
msg-type	Message type.	string	Maximum length: 28	

## config system replacemsg nac-quar

Replacement messages.

```
config system replacemsg nac-quar
  Description: Replacement messages.
  edit <msg-type>
    set buffer {var-string}
    set format [none|text|...]
    set header [none|http|...]
  next
end
```

## config system replacemsg nac-quar

Parameter	Description	Type	Size	Default
buffer	Message string.	var-string	Maximum length: 32768	
format	Format flag.	option	-	
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	No format type.		
	<i>text</i>	Text format.		
	<i>html</i>	HTML format.		
header	Header flag.	option	-	
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	No header type.		
	<i>http</i>	HTTP		
	<i>8bit</i>	8 bit.		

Parameter	Description	Type	Size	Default
msg-type	Message type.	string	Maximum length: 28	

## config system replacemsg spam

Replacement messages.

```
config system replacemsg spam
    Description: Replacement messages.
    edit <msg-type>
        set buffer {var-string}
        set format [none|text|...]
        set header [none|http|...]
    next
end
```

## config system replacemsg spam

Parameter	Description	Type	Size	Default
buffer	Message string.	var-string	Maximum length: 32768	
format	Format flag.	option	-	
	OptionDescription			
	none	No format type.		
	text	Text format.		
	html	HTML format.		
header	Header flag.	option	-	
	OptionDescription			
	none	No header type.		
	http	HTTP		
	8bit	8 bit.		
msg-type	Message type.	string	Maximum length: 28	

## config system replacemsg sslvpn

Replacement messages.

```

config system replacemsg sslvpn
  Description: Replacement messages.
  edit <msg-type>
    set buffer {var-string}
    set format [none|text|...]
    set header [none|http|...]
  next
end

```

## config system replacemsg sslvpn

Parameter	Description	Type	Size	Default
buffer	Message string.	var-string	Maximum length: 32768	
format	Format flag.	option	-	
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	No format type.		
	<i>text</i>	Text format.		
	<i>html</i>	HTML format.		
header	Header flag.	option	-	
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	No header type.		
	<i>http</i>	HTTP		
	<i>8bit</i>	8 bit.		
msg-type	Message type.	string	Maximum length: 28	

## config system replacemsg traffic-quota

Replacement messages.

```

config system replacemsg traffic-quota
  Description: Replacement messages.
  edit <msg-type>
    set buffer {var-string}
    set format [none|text|...]
    set header [none|http|...]
  next
end

```

## config system replacemsg traffic-quota

Parameter	Description	Type	Size	Default								
buffer	Message string.	var-string	Maximum length: 32768									
format	Format flag.	option	-									
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>No format type.</td></tr><tr><td><i>text</i></td><td>Text format.</td></tr><tr><td><i>html</i></td><td>HTML format.</td></tr></table>				Option	Description	<i>none</i>	No format type.	<i>text</i>	Text format.	<i>html</i>	HTML format.
	Option	Description										
	<i>none</i>	No format type.										
	<i>text</i>	Text format.										
<i>html</i>	HTML format.											
header	Header flag.	option	-									
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>No header type.</td></tr><tr><td><i>http</i></td><td>HTTP</td></tr><tr><td><i>8bit</i></td><td>8 bit.</td></tr></table>				Option	Description	<i>none</i>	No header type.	<i>http</i>	HTTP	<i>8bit</i>	8 bit.
	Option	Description										
	<i>none</i>	No header type.										
	<i>http</i>	HTTP										
<i>8bit</i>	8 bit.											
msg-type	Message type.	string	Maximum length: 28									

## config system replacemsg utm

Replacement messages.

```
config system replacemsg utm
  Description: Replacement messages.
  edit <msg-type>
    set buffer {var-string}
    set format [none|text|...]
    set header [none|http|...]
  next
end
```

## config system replacemsg utm

Parameter	Description	Type	Size	Default
buffer	Message string.	var-string	Maximum length: 32768	

Parameter	Description	Type	Size	Default
format	Format flag.	option	-	
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	No format type.		
	<i>text</i>	Text format.		
	<i>html</i>	HTML format.		
header	Header flag.	option	-	
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	No header type.		
	<i>http</i>	HTTP		
	<i>8bit</i>	8 bit.		
msg-type	Message type.	string	Maximum length: 28	

## config system replacemsg webproxy

Replacement messages.

```
config system replacemsg webproxy
  Description: Replacement messages.
  edit <msg-type>
    set buffer {var-string}
    set format [none|text|...]
    set header [none|http|...]
  next
end
```

## config system replacemsg webproxy

Parameter	Description	Type	Size	Default
buffer	Message string.	var-string	Maximum length: 32768	
format	Format flag.	option	-	
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	No format type.		



Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>text</i>	Text format.		
	<i>html</i>	HTML format.		
header	Header flag.	option	-	
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	No header type.		
	<i>http</i>	HTTP		
	<i>8bit</i>	8 bit.		
msg-type	Message type.	string	Maximum length: 28	

## config system resource-limits

Configure resource limits.

```

config system resource-limits
    Description: Configure resource limits.
    set custom-service {integer}
    set dialup-tunnel {integer}
    set firewall-address {integer}
    set firewall-addrgrp {integer}
    set firewall-policy {integer}
    set ipsec-phase1 {integer}
    set ipsec-phase1-interface {integer}
    set ipsec-phase2 {integer}
    set ipsec-phase2-interface {integer}
    set log-disk-quota {integer}
    set onetime-schedule {integer}
    set proxy {integer}
    set recurring-schedule {integer}
    set service-group {integer}
    set session {integer}
    set sslvpn {integer}
    set user {integer}
    set user-group {integer}
end

```

## config system resource-limits

Parameter	Description	Type	Size	Default
custom-service	Maximum number of firewall custom services.	integer	Minimum value: 0 Maximum value: 4294967295	
dialup-tunnel	Maximum number of dial-up tunnels.	integer	Minimum value: 0 Maximum value: 4294967295	
firewall-address	Maximum number of firewall addresses (IPv4, IPv6, multicast).	integer	Minimum value: 0 Maximum value: 4294967295	
firewall-addrgp	Maximum number of firewall address groups (IPv4, IPv6).	integer	Minimum value: 0 Maximum value: 4294967295	
firewall-policy	Maximum number of firewall policies (policy, DoS-policy4, DoS-policy6, multicast).	integer	Minimum value: 0 Maximum value: 4294967295	
ipsec-phase1	Maximum number of VPN IPsec phase1 tunnels.	integer	Minimum value: 0 Maximum value: 4294967295	
ipsec-phase1-interface	Maximum number of VPN IPsec phase1 interface tunnels.	integer	Minimum value: 0 Maximum value: 4294967295	
ipsec-phase2	Maximum number of VPN IPsec phase2 tunnels.	integer	Minimum value: 0 Maximum value: 4294967295	

Parameter	Description	Type	Size	Default
ipsec-phase2-interface	Maximum number of VPN IPsec phase2 interface tunnels.	integer	Minimum value: 0 Maximum value: 4294967295	
log-disk-quota	Log disk quota in megabytes (MB).	integer	Minimum value: 0 Maximum value: 4294967295 **	0
onetime-schedule	Maximum number of firewall one-time schedules.	integer	Minimum value: 0 Maximum value: 4294967295	
proxy	Maximum number of concurrent proxy users.	integer	Minimum value: 0 Maximum value: 4294967295	
recurring-schedule	Maximum number of firewall recurring schedules.	integer	Minimum value: 0 Maximum value: 4294967295	
service-group	Maximum number of firewall service groups.	integer	Minimum value: 0 Maximum value: 4294967295	
session	Maximum number of sessions.	integer	Minimum value: 0 Maximum value: 4294967295	
sslvpn	Maximum number of SSL-VPN.	integer	Minimum value: 0 Maximum value: 4294967295	

Parameter	Description	Type	Size	Default
user	Maximum number of local users.	integer	Minimum value: 0 Maximum value: 4294967295	
user-group	Maximum number of user groups.	integer	Minimum value: 0 Maximum value: 4294967295	

\*\* Values may differ between models.

## config system saml

Global settings for SAML authentication.

```

config system saml
    Description: Global settings for SAML authentication.
    set binding-protocol [post|redirect]
    set cert {string}
    set default-login-page [normal|sso]
    set default-profile {string}
    set entity-id {string}
    set idp-cert {string}
    set idp-entity-id {string}
    set idp-single-logout-url {string}
    set idp-single-sign-on-url {string}
    set life {integer}
    set portal-url {string}
    set role [identity-provider|service-provider]
    set server-address {string}
    config service-providers
        Description: Authorized service providers.
        edit <name>
            set prefix {string}
            set sp-binding-protocol [post|redirect]
            set sp-cert {string}
            set sp-entity-id {string}
            set sp-single-sign-on-url {string}
            set sp-single-logout-url {string}
            set sp-portal-url {string}
            set idp-entity-id {string}
            set idp-single-sign-on-url {string}
            set idp-single-logout-url {string}
            config assertion-attributes
                Description: Customized SAML attributes to send along with assertion.
                edit <name>
                    set type [username|email|...]
                next
            end
        end
    end

```

```

        next
    end
    set single-logout-url {string}
    set single-sign-on-url {string}
    set status [enable|disable]
    set tolerance {integer}
end

```

## config system saml

Parameter	Description	Type	Size	Default						
binding-protocol	IdP Binding protocol.	option	-	redirect						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>post</i></td><td>HTTP POST binding.</td></tr><tr><td><i>redirect</i></td><td>HTTP Redirect binding.</td></tr></table>	Option	Description	<i>post</i>	HTTP POST binding.	<i>redirect</i>	HTTP Redirect binding.			
Option	Description									
<i>post</i>	HTTP POST binding.									
<i>redirect</i>	HTTP Redirect binding.									
cert	Certificate to sign SAML messages.	string	Maximum length: 35							
default-login-page	Choose default login page.	option	-	normal						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>normal</i></td><td>Use local login page as default.</td></tr><tr><td><i>sso</i></td><td>Use IdP's Single Sign-On page as default.</td></tr></table>	Option	Description	<i>normal</i>	Use local login page as default.	<i>sso</i>	Use IdP's Single Sign-On page as default.			
Option	Description									
<i>normal</i>	Use local login page as default.									
<i>sso</i>	Use IdP's Single Sign-On page as default.									
default-profile	Default profile for new SSO admin.	string	Maximum length: 35							
entity-id	SP entity ID.	string	Maximum length: 255							
idp-cert	IDP certificate name.	string	Maximum length: 35							
idp-entity-id	IDP entity ID.	string	Maximum length: 255							
idp-single-logout-url	IDP single logout URL.	string	Maximum length: 255							
idp-single-sign-on-url	IDP single sign-on URL.	string	Maximum length: 255							

Parameter	Description	Type	Size	Default						
life	Length of the range of time when the assertion is valid (in minutes).	integer	Minimum value: 0 Maximum value: 4294967295	30						
portal-url	SP portal URL.	string	Maximum length: 255							
role	SAML role.	option	-	service-provider						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>identity-provider</i></td><td>Identity Provider.</td></tr><tr><td><i>service-provider</i></td><td>Service Provider.</td></tr></table>				Option	Description	<i>identity-provider</i>	Identity Provider.	<i>service-provider</i>	Service Provider.
	Option	Description								
	<i>identity-provider</i>	Identity Provider.								
<i>service-provider</i>	Service Provider.									
server-address	Server address.	string	Maximum length: 63							
single-logout-url	SP single logout URL.	string	Maximum length: 255							
single-sign-on-url	SP single sign-on URL.	string	Maximum length: 255							
status	Enable/disable SAML authentication.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable SAML authentication.</td></tr><tr><td><i>disable</i></td><td>Disable SAML authentication.</td></tr></table>				Option	Description	<i>enable</i>	Enable SAML authentication.	<i>disable</i>	Disable SAML authentication.
	Option	Description								
	<i>enable</i>	Enable SAML authentication.								
<i>disable</i>	Disable SAML authentication.									
tolerance	Tolerance to the range of time when the assertion is valid (in minutes).	integer	Minimum value: 0 Maximum value: 4294967295	5						

### config service-providers

Parameter	Description	Type	Size	Default
name	Name.	string	Maximum length: 35	
prefix	Prefix.	string	Maximum length: 35	
sp-binding-protocol	SP binding protocol.	option	-	post

Parameter	Description	Type	Size	Default
	Option Description			
	<i>post</i>	HTTP POST binding.		
	<i>redirect</i>	HTTP Redirect binding.		
sp-cert	SP certificate name.	string	Maximum length: 35	
sp-entity-id	SP entity ID.	string	Maximum length: 255	
sp-single-sign-on-url	SP single sign-on URL.	string	Maximum length: 255	
sp-single-logout-url	SP single logout URL.	string	Maximum length: 255	
sp-portal-url	SP portal URL.	string	Maximum length: 255	
idp-entity-id	IDP entity ID.	string	Maximum length: 255	
idp-single-sign-on-url	IDP single sign-on URL.	string	Maximum length: 255	
idp-single-logout-url	IDP single logout URL.	string	Maximum length: 255	

#### config assertion-attributes

Parameter	Description	Type	Size	Default
name	Name.	string	Maximum length: 35	
type	Type.	option	-	username
	Option Description			
	<i>username</i>	User Name.		
	<i>email</i>	Email Address.		
	<i>profile-name</i>	Profile Name.		

## config system sdn-connector

Configure connection to SDN Connector.

```
config system sdn-connector
    Description: Configure connection to SDN Connector.
```

```

edit <name>
    set access-key {string}
    set api-key {password}
    set azure-region [global|china|...]
    set client-id {string}
    set client-secret {password}
    set compartment-id {string}
    set compute-generation {integer}
    set domain {string}
    config external-account-list
        Description: Configure AWS external account list.
        edit <role-arn>
            set external-id {string}
            set region-list <region1>, <region2>, ...
        next
    end
    config external-ip
        Description: Configure GCP external IP.
        edit <name>
            next
        end
    config forwarding-rule
        Description: Configure GCP forwarding rule.
        edit <rule-name>
            set target {string}
        next
    end
    config gcp-project-list
        Description: Configure GCP project list.
        edit <id>
            set gcp-zone-list <name1>, <name2>, ...
        next
    end
    set group-name {string}
    set ha-status [disable|enable]
    set ibm-region [dallas|washington-dc|...]
    set login-endpoint {string}
    config nic
        Description: Configure Azure network interface.
        edit <name>
            config ip
                Description: Configure IP configuration.
                edit <name>
                    set public-ip {string}
                    set resource-group {string}
                next
            end
        next
    end
    set oci-cert {string}
    set oci-fingerprint {string}
    set oci-region {string}
    set oci-region-type [commercial|government]
    set password {password_aes256}
    set private-key {user}
    set region {string}

```



```

set resource-group {string}
set resource-url {string}
config route
    Description: Configure GCP route.
    edit <name>
    next
end
config route-table
    Description: Configure Azure route table.
    edit <name>
        set subscription-id {string}
        set resource-group {string}
        config route
            Description: Configure Azure route.
            edit <name>
                set next-hop {string}
            next
        end
    next
end
set secret-key {password}
set secret-token {user}
set server {string}
set server-list <ip1>, <ip2>, ...
set server-port {integer}
set service-account {string}
set status [disable|enable]
set subscription-id {string}
set tenant-id {string}
set type [aci|alicloud|...]
set update-interval {integer}
set use-metadata-iam [disable|enable]
set user-id {string}
set username {string}
set vcenter-password {password_aes256}
set vcenter-server {string}
set vcenter-username {string}
set verify-certificate [disable|enable]
set vpc-id {string}
next
end

```

## config system sdn-connector

Parameter	Description	Type	Size	Default
access-key	AWS / ACS access key ID.	string	Maximum length: 31	
api-key	IBM cloud API key or service ID API key.	password	Not Specified	
azure-region	Azure server region.	option	-	global

Parameter	Description	Type	Size	Default												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>global</i></td><td>Global Azure Server.</td></tr><tr><td><i>china</i></td><td>China Azure Server.</td></tr><tr><td><i>germany</i></td><td>Germany Azure Server.</td></tr><tr><td><i>usgov</i></td><td>US Government Azure Server.</td></tr><tr><td><i>local</i></td><td>Azure Stack Local Server.</td></tr></table>	Option	Description	<i>global</i>	Global Azure Server.	<i>china</i>	China Azure Server.	<i>germany</i>	Germany Azure Server.	<i>usgov</i>	US Government Azure Server.	<i>local</i>	Azure Stack Local Server.			
	Option	Description														
	<i>global</i>	Global Azure Server.														
	<i>china</i>	China Azure Server.														
	<i>germany</i>	Germany Azure Server.														
	<i>usgov</i>	US Government Azure Server.														
<i>local</i>	Azure Stack Local Server.															
client-id	Azure client ID (application ID).	string	Maximum length: 63													
client-secret	Azure client secret (application key).	password	Not Specified													
compartment-id	Compartment ID.	string	Maximum length: 127													
compute-generation	Compute generation for IBM cloud infrastructure.	integer	Minimum value: 1 Maximum value: 2	2												
domain	Domain name.	string	Maximum length: 127													
group-name	Group name of computers.	string	Maximum length: 127													
ha-status	Enable/disable use for FortiGate HA service.	option	-	disable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable use for FortiGate HA service.</td></tr><tr><td><i>enable</i></td><td>Enable use for FortiGate HA service.</td></tr></table>	Option	Description	<i>disable</i>	Disable use for FortiGate HA service.	<i>enable</i>	Enable use for FortiGate HA service.									
	Option	Description														
	<i>disable</i>	Disable use for FortiGate HA service.														
<i>enable</i>	Enable use for FortiGate HA service.															
ibm-region	IBM cloud region name.	option	-	dallas												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>dallas</i></td><td>US South (Dallas) Public Endpoint.</td></tr><tr><td><i>washington-dc</i></td><td>US East (Washington DC) Public Endpoint.</td></tr><tr><td><i>london</i></td><td>United Kingdom (London) Public Endpoint.</td></tr><tr><td><i>frankfurt</i></td><td>Germany (Frankfurt) Public Endpoint.</td></tr><tr><td><i>sydney</i></td><td>Australia (Sydney) Public Endpoint.</td></tr></table>	Option	Description	<i>dallas</i>	US South (Dallas) Public Endpoint.	<i>washington-dc</i>	US East (Washington DC) Public Endpoint.	<i>london</i>	United Kingdom (London) Public Endpoint.	<i>frankfurt</i>	Germany (Frankfurt) Public Endpoint.	<i>sydney</i>	Australia (Sydney) Public Endpoint.			
	Option	Description														
	<i>dallas</i>	US South (Dallas) Public Endpoint.														
	<i>washington-dc</i>	US East (Washington DC) Public Endpoint.														
	<i>london</i>	United Kingdom (London) Public Endpoint.														
	<i>frankfurt</i>	Germany (Frankfurt) Public Endpoint.														
<i>sydney</i>	Australia (Sydney) Public Endpoint.															

Parameter	Description	Type	Size	Default										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>tokyo</i></td><td>Japan (Tokyo) Public Endpoint.</td></tr><tr><td><i>osaka</i></td><td>Japan (Osaka) Public Endpoint.</td></tr><tr><td><i>toronto</i></td><td>Canada (Toronto) Public Endpoint.</td></tr><tr><td><i>sao-paulo</i></td><td>Brazil (Sao Paulo) Public Endpoint.</td></tr></table>	Option	Description	<i>tokyo</i>	Japan (Tokyo) Public Endpoint.	<i>osaka</i>	Japan (Osaka) Public Endpoint.	<i>toronto</i>	Canada (Toronto) Public Endpoint.	<i>sao-paulo</i>	Brazil (Sao Paulo) Public Endpoint.			
	Option	Description												
	<i>tokyo</i>	Japan (Tokyo) Public Endpoint.												
	<i>osaka</i>	Japan (Osaka) Public Endpoint.												
	<i>toronto</i>	Canada (Toronto) Public Endpoint.												
<i>sao-paulo</i>	Brazil (Sao Paulo) Public Endpoint.													
login-endpoint	Azure Stack login endpoint.	string	Maximum length: 127											
name	SDN connector name.	string	Maximum length: 35											
oci-cert	OCI certificate.	string	Maximum length: 63											
oci-fingerprint	OCI pubkey fingerprint.	string	Maximum length: 63											
oci-region	OCI server region.	string	Maximum length: 31											
oci-region-type	OCI region type.	option	-	commercial										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>commercial</i></td><td>Commercial region.</td></tr><tr><td><i>government</i></td><td>Government region.</td></tr></table>	Option	Description	<i>commercial</i>	Commercial region.	<i>government</i>	Government region.							
	Option	Description												
	<i>commercial</i>	Commercial region.												
<i>government</i>	Government region.													
password	Password of the remote SDN connector as login credentials.	password_aes256	Not Specified											
private-key	Private key of GCP service account.	user	Not Specified											
region	AWS / ACS region name.	string	Maximum length: 31											
resource-group	Azure resource group.	string	Maximum length: 63											
resource-url	Azure Stack resource URL.	string	Maximum length: 127											
secret-key	AWS / ACS secret access key.	password	Not Specified											
secret-token	Secret token of Kubernetes service account.	user	Not Specified											

Parameter	Description	Type	Size	Default																						
server	Server address of the remote SDN connector.	string	Maximum length: 127																							
server-list <ip>	Server address list of the remote SDN connector. IPv4 address.	string	Maximum length: 15																							
server-port	Port number of the remote SDN connector.	integer	Minimum value: 0 Maximum value: 65535	0																						
service-account	GCP service account email.	string	Maximum length: 127																							
status	Enable/disable connection to the remote SDN connector.	option	-	enable																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable connection to this SDN Connector.</td></tr><tr><td>enable</td><td>Enable connection to this SDN Connector.</td></tr></table>				Option	Description	disable	Disable connection to this SDN Connector.	enable	Enable connection to this SDN Connector.																
Option	Description																									
disable	Disable connection to this SDN Connector.																									
enable	Enable connection to this SDN Connector.																									
subscription-id	Azure subscription ID.	string	Maximum length: 63																							
tenant-id	Tenant ID (directory ID).	string	Maximum length: 127																							
type	Type of SDN connector.	option	-	aws																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>aci</td><td>Application Centric Infrastructure (ACI).</td></tr><tr><td>alicloud</td><td>AliCloud Service (ACS).</td></tr><tr><td>aws</td><td>Amazon Web Services (AWS).</td></tr><tr><td>azure</td><td>Microsoft Azure.</td></tr><tr><td>gcp</td><td>Google Cloud Platform (GCP).</td></tr><tr><td>nsx</td><td>VMware NSX.</td></tr><tr><td>nuage</td><td>Nuage VSP.</td></tr><tr><td>oci</td><td>Oracle Cloud Infrastructure.</td></tr><tr><td>openstack</td><td>OpenStack.</td></tr><tr><td>kubernetes</td><td>Kubernetes.</td></tr></table>				Option	Description	aci	Application Centric Infrastructure (ACI).	alicloud	AliCloud Service (ACS).	aws	Amazon Web Services (AWS).	azure	Microsoft Azure.	gcp	Google Cloud Platform (GCP).	nsx	VMware NSX.	nuage	Nuage VSP.	oci	Oracle Cloud Infrastructure.	openstack	OpenStack.	kubernetes	Kubernetes.
Option	Description																									
aci	Application Centric Infrastructure (ACI).																									
alicloud	AliCloud Service (ACS).																									
aws	Amazon Web Services (AWS).																									
azure	Microsoft Azure.																									
gcp	Google Cloud Platform (GCP).																									
nsx	VMware NSX.																									
nuage	Nuage VSP.																									
oci	Oracle Cloud Infrastructure.																									
openstack	OpenStack.																									
kubernetes	Kubernetes.																									

Parameter	Description	Type	Size	Default													
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>vmware</i></td><td>VMware vSphere (vCenter &amp; ESXi).</td></tr><tr><td><i>sepm</i></td><td>Symantec Endpoint Protection Manager.</td></tr><tr><td><i>aci-direct</i></td><td>Application Centric Infrastructure (ACI Direct Connection).</td></tr><tr><td><i>ibm</i></td><td>IBM Cloud Infrastructure.</td></tr><tr><td><i>nutanix</i></td><td>Nutanix Prism Central.</td></tr></table>		Option	Description	<i>vmware</i>	VMware vSphere (vCenter & ESXi).	<i>sepm</i>	Symantec Endpoint Protection Manager.	<i>aci-direct</i>	Application Centric Infrastructure (ACI Direct Connection).	<i>ibm</i>	IBM Cloud Infrastructure.	<i>nutanix</i>	Nutanix Prism Central.			
	Option	Description															
	<i>vmware</i>	VMware vSphere (vCenter & ESXi).															
	<i>sepm</i>	Symantec Endpoint Protection Manager.															
	<i>aci-direct</i>	Application Centric Infrastructure (ACI Direct Connection).															
	<i>ibm</i>	IBM Cloud Infrastructure.															
<i>nutanix</i>	Nutanix Prism Central.																
update-interval	Dynamic object update interval.	integer	Minimum value: 0 Maximum value: 3600	60													
use-metadata-iam	Enable/disable use of IAM role from metadata to call API.	option	-	disable													
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable using IAM role to call API.</td></tr><tr><td><i>enable</i></td><td>Enable using IAM role to call API.</td></tr></table>		Option	Description	<i>disable</i>	Disable using IAM role to call API.	<i>enable</i>	Enable using IAM role to call API.									
	Option	Description															
	<i>disable</i>	Disable using IAM role to call API.															
<i>enable</i>	Enable using IAM role to call API.																
user-id	User ID.	string	Maximum length: 127														
username	Username of the remote SDN connector as login credentials.	string	Maximum length: 64														
vcenter-password	vCenter server password for NSX quarantine.	password_aes256	Not Specified														
vcenter-server	vCenter server address for NSX quarantine.	string	Maximum length: 127														
vcenter-username	vCenter server username for NSX quarantine.	string	Maximum length: 64														
verify-certificate	Enable/disable server certificate verification.	option	-	enable													
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable server certificate verification.</td></tr><tr><td><i>enable</i></td><td>Enable server certificate verification.</td></tr></table>		Option	Description	<i>disable</i>	Disable server certificate verification.	<i>enable</i>	Enable server certificate verification.									
	Option	Description															
	<i>disable</i>	Disable server certificate verification.															
<i>enable</i>	Enable server certificate verification.																
vpc-id	AWS VPC ID.	string	Maximum length: 31														

### config external-account-list

Parameter	Description	Type	Size	Default
role-arn	AWS role ARN to assume.	string	Maximum length: 2047	
external-id	AWS external ID.	string	Maximum length: 1399	
region-list <region>	AWS region name list. AWS region name.	string	Maximum length: 31	

### config external-ip

Parameter	Description	Type	Size	Default
name	External IP name.	string	Maximum length: 63	

### config forwarding-rule

Parameter	Description	Type	Size	Default
rule-name	Forwarding rule name.	string	Maximum length: 63	
target	Target instance name.	string	Maximum length: 63	

### config gcp-project-list

Parameter	Description	Type	Size	Default
id	GCP project ID.	string	Maximum length: 127	
gcp-zone-list <name>	Configure GCP zone list. GCP zone name.	string	Maximum length: 127	

### config nic

Parameter	Description	Type	Size	Default
name	Network interface name.	string	Maximum length: 63	

### config ip

Parameter	Description	Type	Size	Default
name	IP configuration name.	string	Maximum length: 63	
public-ip	Public IP name.	string	Maximum length: 63	
resource-group	Resource group of Azure public IP.	string	Maximum length: 63	

### config route

Parameter	Description	Type	Size	Default
name	Route name.	string	Maximum length: 63	

### config route

Parameter	Description	Type	Size	Default
name	Route name.	string	Maximum length: 63	
next-hop	Next hop address.	string	Maximum length: 127	

### config route-table

Parameter	Description	Type	Size	Default
name	Route table name.	string	Maximum length: 63	
subscription-id	Subscription ID of Azure route table.	string	Maximum length: 63	
resource-group	Resource group of Azure route table.	string	Maximum length: 63	

### config route

Parameter	Description	Type	Size	Default
name	Route name.	string	Maximum length: 63	

## config route

Parameter	Description	Type	Size	Default
name	Route name.	string	Maximum length: 63	
next-hop	Next hop address.	string	Maximum length: 127	

## config system sdwan

Configure redundant Internet connections with multiple outbound links and health-check profiles.

```
config system sdwan
    Description: Configure redundant Internet connections with multiple outbound links and
health-check profiles.
    config duplication
        Description: Create SD-WAN duplication rule.
        edit <id>
            set service-id <id1>, <id2>, ...
            set srcaddr <name1>, <name2>, ...
            set dstaddr <name1>, <name2>, ...
            set srcaddr6 <name1>, <name2>, ...
            set dstaddr6 <name1>, <name2>, ...
            set srcintf <name1>, <name2>, ...
            set dstintf <name1>, <name2>, ...
            set service <name1>, <name2>, ...
            set packet-duplication [disable|force|...]
            set packet-de-duplication [enable|disable]
        next
    end
    set duplication-max-num {integer}
    set fail-alert-interfaces <name1>, <name2>, ...
    set fail-detect [enable|disable]
    config health-check
        Description: SD-WAN status checking or health checking. Identify a server on the
Internet and determine how SD-WAN verifies that the FortiGate can communicate with it.
        edit <name>
            set probe-packets [disable|enable]
            set addr-mode [ipv4|ipv6]
            set system-dns [disable|enable]
            set server {string}
            set detect-mode [active|passive|...]
            set protocol [ping|tcp-echo|...]
            set port {integer}
            set quality-measured-method [half-open|half-close]
            set security-mode [none|authentication]
            set user {string}
            set password {password}
            set packet-size {integer}
            set ha-priority {integer}
            set ftp-mode [passive|port]
            set ftp-file {string}
```



```

set http-get {string}
set http-agent {string}
set http-match {string}
set dns-request-domain {string}
set dns-match-ip {ipv4-address}
set interval {integer}
set probe-timeout {integer}
set failtime {integer}
set recoverytime {integer}
set probe-count {integer}
set diffservcode {user}
set update-cascade-interface [enable|disable]
set update-static-route [enable|disable]
set sla-fail-log-period {integer}
set sla-pass-log-period {integer}
set threshold-warning-packetloss {integer}
set threshold-alert-packetloss {integer}
set threshold-warning-latency {integer}
set threshold-alert-latency {integer}
set threshold-warning-jitter {integer}
set threshold-alert-jitter {integer}
set members <seq-num1>, <seq-num2>, ...
config sla
    Description: Service level agreement (SLA).
    edit <id>
        set link-cost-factor {option1}, {option2}, ...
        set latency-threshold {integer}
        set jitter-threshold {integer}
        set packetloss-threshold {integer}
    next
end
next
end
set load-balance-mode [source-ip-based|weight-based|...]
config members
    Description: FortiGate interfaces added to the SD-WAN.
    edit <seq-num>
        set interface {string}
        set zone {string}
        set gateway {ipv4-address}
        set source {ipv4-address}
        set gateway6 {ipv6-address}
        set source6 {ipv6-address}
        set cost {integer}
        set weight {integer}
        set priority {integer}
        set priority6 {integer}
        set spillover-threshold {integer}
        set ingress-spillover-threshold {integer}
        set volume-ratio {integer}
        set status [disable|enable]
        set comment {var-string}
    next
end
config neighbor
    Description: Create SD-WAN neighbor from BGP neighbor table to control route

```

---

advertisements according to SLA status.

```
edit <ip>
    set member {integer}
    set mode [sla|speedtest]
    set role [standalone|primary|...]
    set health-check {string}
    set sla-id {integer}
next
end
set neighbor-hold-boot-time {integer}
set neighbor-hold-down [enable|disable]
set neighbor-hold-down-time {integer}
config service
```

Description: Create SD-WAN rules (also called services) to control how sessions are distributed to interfaces in the SD-WAN.

```
edit <id>
    set name {string}
    set addr-mode [ipv4|ipv6]
    set input-device <name1>, <name2>, ...
    set input-device-negate [enable|disable]
    set mode [auto|manual|...]
    set minimum-sla-meet-members {integer}
    set hash-mode [round-robin|source-ip-based|...]
    set role [standalone|primary|...]
    set standalone-action [enable|disable]
    set quality-link {integer}
    set tos {user}
    set tos-mask {user}
    set protocol {integer}
    set start-port {integer}
    set end-port {integer}
    set route-tag {integer}
    set dst <name1>, <name2>, ...
    set dst-negate [enable|disable]
    set src <name1>, <name2>, ...
    set dst6 <name1>, <name2>, ...
    set src6 <name1>, <name2>, ...
    set src-negate [enable|disable]
    set users <name1>, <name2>, ...
    set groups <name1>, <name2>, ...
    set internet-service [enable|disable]
    set internet-service-custom <name1>, <name2>, ...
    set internet-service-custom-group <name1>, <name2>, ...
    set internet-service-name <name1>, <name2>, ...
    set internet-service-group <name1>, <name2>, ...
    set internet-service-app-ctrl <id1>, <id2>, ...
    set internet-service-app-ctrl-group <name1>, <name2>, ...
    set health-check <name1>, <name2>, ...
    set link-cost-factor [latency|jitter|...]
    set packet-loss-weight {integer}
    set latency-weight {integer}
    set jitter-weight {integer}
    set bandwidth-weight {integer}
    set link-cost-threshold {integer}
    set hold-down-time {integer}
    set dscp-forward [enable|disable]
```

```

set dscp-reverse [enable|disable]
set dscp-forward-tag {user}
set dscp-reverse-tag {user}
config sla
    Description: Service level agreement (SLA).
    edit <health-check>
        set id {integer}
    next
end
set priority-members <seq-num1>, <seq-num2>, ...
set priority-zone <name1>, <name2>, ...
set status [enable|disable]
set gateway [enable|disable]
set default [enable|disable]
set sla-compare-method [order|number]
set tie-break [zone|cfg-order|...]
set use-shortcut-sla [enable|disable]
set passive-measurement [enable|disable]
next
end
set speedtest-bypass-routing [disable|enable]
set status [disable|enable]
config zone
    Description: Configure SD-WAN zones.
    edit <name>
        set service-sla-tie-break [cfg-order|fib-best-match]
    next
end
end

```

## config system sdwan

Parameter	Description	Type	Size	Default						
duplication-max-num	Maximum number of interface members a packet is duplicated in the SD-WAN zone.	integer	Minimum value: 2 Maximum value: 4	2						
fail-alert-interfaces <name>	Physical interfaces that will be alerted. Physical interface name.	string	Maximum length: 79							
fail-detect	Enable/disable SD-WAN Internet connection status checking (failure detection).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable status checking.</td></tr><tr><td><i>disable</i></td><td>Disable status checking.</td></tr></table>				Option	Description	<i>enable</i>	Enable status checking.	<i>disable</i>	Disable status checking.
Option	Description									
<i>enable</i>	Enable status checking.									
<i>disable</i>	Disable status checking.									
load-balance-mode	Algorithm or mode to use for load balancing Internet traffic to SD-WAN members.	option	-	source-ip-based						

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>source-ip-based</i>	Source IP load balancing. All traffic from a source IP is sent to the same interface.		
	<i>weight-based</i>	Weight-based load balancing. Interfaces with higher weights have higher priority and get more traffic.		
	<i>usage-based</i>	Usage-based load balancing. All traffic is sent to the first interface on the list. When the bandwidth on that interface exceeds the spill-over limit new traffic is sent to the next interface.		
	<i>source-dest-ip-based</i>	Source and destination IP load balancing. All traffic from a source IP to a destination IP is sent to the same interface.		
	<i>measured-volume-based</i>	Volume-based load balancing. Traffic is load balanced based on traffic volume (in bytes). More traffic is sent to interfaces with higher volume ratios.		
neighbor-hold-boot-time	Waiting period in seconds when switching from the primary neighbor to the secondary neighbor from the neighbor start..	integer	Minimum value: 0 Maximum value: 10000000	0
neighbor-hold-down	Enable/disable hold switching from the secondary neighbor to the primary neighbor.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable hold switching from the secondary neighbor to the primary neighbor.		
	<i>disable</i>	Disable hold switching from the secondary neighbor to the primary neighbor.		
neighbor-hold-down-time	Waiting period in seconds when switching from the secondary neighbor to the primary neighbor when hold-down is disabled..	integer	Minimum value: 0 Maximum value: 10000000	0
speedtest-bypass-routing	Enable/disable bypass routing when speedtest on a SD-WAN member.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable SD-WAN.		
	<i>enable</i>	Enable SD-WAN.		
status	Enable/disable SD-WAN.	option	-	disable

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable SD-WAN.		
	<i>enable</i>	Enable SD-WAN.		

## config duplication

Parameter	Description	Type	Size	Default
id	Duplication rule ID.	integer	Minimum value: 1 Maximum value: 255	0
service-id <id>	SD-WAN service rule ID list. SD-WAN service rule ID.	integer	Minimum value: 0 Maximum value: 4294967295	
srcaddr <name>	Source address or address group names. Address or address group name.	string	Maximum length: 79	
dstaddr <name>	Destination address or address group names. Address or address group name.	string	Maximum length: 79	
srcaddr6 <name>	Source address6 or address6 group names. Address6 or address6 group name.	string	Maximum length: 79	
dstaddr6 <name>	Destination address6 or address6 group names. Address6 or address6 group name.	string	Maximum length: 79	
srcintf <name>	Incoming (ingress) interfaces or zones. Interface, zone or SDWAN zone name.	string	Maximum length: 79	
dstintf <name>	Outgoing (egress) interfaces or zones. Interface, zone or SDWAN zone name.	string	Maximum length: 79	
service <name>	Service and service group name. Service and service group name.	string	Maximum length: 79	
packet-duplication	Configure packet duplication method.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable packet duplication.		
	<i>force</i>	Duplicate packets across all interface members of the SD-WAN zone.		

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>on-demand</i>	Duplicate packets across all interface members of the SD-WAN zone based on the link quality.		
packet-de-duplication	Enable/disable discarding of packets that have been duplicated.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable discarding of packets that have been duplicated.		
	<i>disable</i>	Disable discarding of packets that have been duplicated.		

### config health-check

Parameter	Description	Type	Size	Default
name	Status check or health check name.	string	Maximum length: 35	
probe-packets	Enable/disable transmission of probe packets.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable transmission of probe packets.		
	<i>enable</i>	Enable transmission of probe packets.		
addr-mode	Address mode (IPv4 or IPv6).	option	-	ipv4
	<b>Option</b>	<b>Description</b>		
	<i>ipv4</i>	IPv4 mode.		
	<i>ipv6</i>	IPv6 mode.		
system-dns	Enable/disable system DNS as the probe server.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable system DNS as the probe server.		
	<i>enable</i>	Enable system DNS as the probe server.		
server	IP address or FQDN name of the server.	string	Maximum length: 79	
detect-mode	The mode determining how to detect the server.	option	-	active

Parameter	Description	Type	Size	Default																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>active</i></td><td>The probes are sent actively.</td></tr><tr><td><i>passive</i></td><td>The traffic measures health without probes.</td></tr><tr><td><i>prefer-passive</i></td><td>The probes are sent in case of no new traffic.</td></tr></table>	Option	Description	<i>active</i>	The probes are sent actively.	<i>passive</i>	The traffic measures health without probes.	<i>prefer-passive</i>	The probes are sent in case of no new traffic.													
	Option	Description																				
	<i>active</i>	The probes are sent actively.																				
	<i>passive</i>	The traffic measures health without probes.																				
<i>prefer-passive</i>	The probes are sent in case of no new traffic.																					
protocol	Protocol used to determine if the FortiGate can communicate with the server.	option	-	ping																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ping</i></td><td>Use PING to test the link with the server.</td></tr><tr><td><i>tcp-echo</i></td><td>Use TCP echo to test the link with the server.</td></tr><tr><td><i>udp-echo</i></td><td>Use UDP echo to test the link with the server.</td></tr><tr><td><i>http</i></td><td>Use HTTP-GET to test the link with the server.</td></tr><tr><td><i>twamp</i></td><td>Use TWAMP to test the link with the server.</td></tr><tr><td><i>dns</i></td><td>Use DNS query to test the link with the server.</td></tr><tr><td><i>tcp-connect</i></td><td>Use a full TCP connection to test the link with the server.</td></tr><tr><td><i>ftp</i></td><td>Use FTP to test the link with the server.</td></tr></table>	Option	Description	<i>ping</i>	Use PING to test the link with the server.	<i>tcp-echo</i>	Use TCP echo to test the link with the server.	<i>udp-echo</i>	Use UDP echo to test the link with the server.	<i>http</i>	Use HTTP-GET to test the link with the server.	<i>twamp</i>	Use TWAMP to test the link with the server.	<i>dns</i>	Use DNS query to test the link with the server.	<i>tcp-connect</i>	Use a full TCP connection to test the link with the server.	<i>ftp</i>	Use FTP to test the link with the server.			
	Option	Description																				
	<i>ping</i>	Use PING to test the link with the server.																				
	<i>tcp-echo</i>	Use TCP echo to test the link with the server.																				
	<i>udp-echo</i>	Use UDP echo to test the link with the server.																				
	<i>http</i>	Use HTTP-GET to test the link with the server.																				
	<i>twamp</i>	Use TWAMP to test the link with the server.																				
	<i>dns</i>	Use DNS query to test the link with the server.																				
	<i>tcp-connect</i>	Use a full TCP connection to test the link with the server.																				
<i>ftp</i>	Use FTP to test the link with the server.																					
port	Port number used to communicate with the server over the selected protocol.	integer	Minimum value: 0 Maximum value: 65535	0																		
quality-measured-method	Method to measure the quality of tcp-connect.	option	-	half-open																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>half-open</i></td><td>Measure the round trip between syn and ack.</td></tr><tr><td><i>half-close</i></td><td>Measure the round trip between fin and ack.</td></tr></table>	Option	Description	<i>half-open</i>	Measure the round trip between syn and ack.	<i>half-close</i>	Measure the round trip between fin and ack.															
	Option	Description																				
	<i>half-open</i>	Measure the round trip between syn and ack.																				
<i>half-close</i>	Measure the round trip between fin and ack.																					
security-mode	Twamp controller security mode.	option	-	none																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>Unauthenticated mode.</td></tr><tr><td><i>authentication</i></td><td>Authenticated mode.</td></tr></table>	Option	Description	<i>none</i>	Unauthenticated mode.	<i>authentication</i>	Authenticated mode.															
	Option	Description																				
	<i>none</i>	Unauthenticated mode.																				
<i>authentication</i>	Authenticated mode.																					

Parameter	Description	Type	Size	Default
user	The user name to access probe server.	string	Maximum length: 64	
password	TWAMP controller password in authentication mode.	password	Not Specified	
packet-size	Packet size of a TWAMP test session.	integer	Minimum value: 64 Maximum value: 1024	64
ha-priority	HA election priority.	integer	Minimum value: 1 Maximum value: 50	1
ftp-mode	FTP mode.	option	-	passive
	Option	Description		
	passive	The FTP health-check initiates and establishes the data connection.		
	port	The FTP server initiates and establishes the data connection.		
ftp-file	Full path and file name on the FTP server to download for FTP health-check to probe.	string	Maximum length: 254	
http-get	URL used to communicate with the server if the protocol is HTTP.	string	Maximum length: 1024	/
http-agent	String in the http-agent field in the HTTP header.	string	Maximum length: 1024	Chrome/ Safari/
http-match	Response string expected from the server if the protocol is HTTP.	string	Maximum length: 1024	
dns-request-domain	Fully qualified domain name to resolve for the DNS probe.	string	Maximum length: 255	www.example.com
dns-match-ip	Response IP expected from DNS server if the protocol is DNS.	ipv4-address	Not Specified	0.0.0.0
interval	Status check interval in milliseconds, or the time between attempting to connect to the server.	integer	Minimum value: 20 Maximum value: 3600000	500



Parameter	Description	Type	Size	Default						
probe-timeout	Time to wait before a probe packet is considered lost.	integer	Minimum value: 20 Maximum value: 3600000	500						
failtime	Number of failures before server is considered lost.	integer	Minimum value: 1 Maximum value: 3600	5						
recoverytime	Number of successful responses received before server is considered recovered.	integer	Minimum value: 1 Maximum value: 3600	5						
probe-count	Number of most recent probes that should be used to calculate latency and jitter.	integer	Minimum value: 5 Maximum value: 30	30						
diffservcode	Differentiated services code point (DSCP) in the IP header of the probe packet.	user	Not Specified							
update-cascade-interface	Enable/disable update cascade interface.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable update cascade interface.</td></tr><tr><td>disable</td><td>Disable update cascade interface.</td></tr></table>				Option	Description	enable	Enable update cascade interface.	disable	Disable update cascade interface.
	Option	Description								
	enable	Enable update cascade interface.								
disable	Disable update cascade interface.									
update-static-route	Enable/disable updating the static route.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable updating the static route.</td></tr><tr><td>disable</td><td>Disable updating the static route.</td></tr></table>				Option	Description	enable	Enable updating the static route.	disable	Disable updating the static route.
	Option	Description								
	enable	Enable updating the static route.								
disable	Disable updating the static route.									
sla-fail-log-period	Time interval in seconds that SLA fail log messages will be generated.	integer	Minimum value: 0 Maximum value: 3600	0						

Parameter	Description	Type	Size	Default
sla-pass-log-period	Time interval in seconds that SLA pass log messages will be generated.	integer	Minimum value: 0 Maximum value: 3600	0
threshold-warning-packetloss	Warning threshold for packet loss.	integer	Minimum value: 0 Maximum value: 100	0
threshold-alert-packetloss	Alert threshold for packet loss.	integer	Minimum value: 0 Maximum value: 100	0
threshold-warning-latency	Warning threshold for latency.	integer	Minimum value: 0 Maximum value: 4294967295	0
threshold-alert-latency	Alert threshold for latency.	integer	Minimum value: 0 Maximum value: 4294967295	0
threshold-warning-jitter	Warning threshold for jitter.	integer	Minimum value: 0 Maximum value: 4294967295	0
threshold-alert-jitter	Alert threshold for jitter.	integer	Minimum value: 0 Maximum value: 4294967295	0
members <seq-num>	Member sequence number list. Member sequence number.	integer	Minimum value: 0 Maximum value: 4294967295	

## config sla

Parameter	Description	Type	Size	Default
health-check	SD-WAN health-check.	string	Maximum length: 35	
id	SLA ID.	integer	Minimum value: 0 Maximum value: 4294967295	0

## config members

Parameter	Description	Type	Size	Default
seq-num	Sequence number.	integer	Minimum value: 0 Maximum value: 512	0
interface	Interface name.	string	Maximum length: 15	
zone	Zone name.	string	Maximum length: 35	virtual-wan-link
gateway	The default gateway for this interface. Usually the default gateway of the Internet service provider that this interface is connected to.	ipv4-address	Not Specified	0.0.0.0
source	Source IP address used in the health-check packet to the server.	ipv4-address	Not Specified	0.0.0.0
gateway6	IPv6 gateway.	ipv6-address	Not Specified	::
source6	Source IPv6 address used in the health-check packet to the server.	ipv6-address	Not Specified	::
cost	Cost of this interface for services in SLA mode.	integer	Minimum value: 0 Maximum value: 4294967295	0
weight	Weight of this interface for weighted load balancing. More traffic is directed to interfaces with higher weights.	integer	Minimum value: 1 Maximum value: 255	1

Parameter	Description	Type	Size	Default						
priority	Priority of the interface for IPv4. Used for SD-WAN rules or priority rules.	integer	Minimum value: 1 Maximum value: 65535	1						
priority6	Priority of the interface for IPv6. Used for SD-WAN rules or priority rules.	integer	Minimum value: 1 Maximum value: 65535	1024						
spillover-threshold	Egress spillover threshold for this interface. When this traffic volume threshold is reached, new sessions spill over to other interfaces in the SD-WAN.	integer	Minimum value: 0 Maximum value: 16776000	0						
ingress-spillover-threshold	Ingress spillover threshold for this interface. When this traffic volume threshold is reached, new sessions spill over to other interfaces in the SD-WAN.	integer	Minimum value: 0 Maximum value: 16776000	0						
volume-ratio	Measured volume ratio.	integer	Minimum value: 1 Maximum value: 255	1						
status	Enable/disable this interface in the SD-WAN.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable this interface in the SD-WAN.</td></tr><tr><td><i>enable</i></td><td>Enable this interface in the SD-WAN.</td></tr></table>				Option	Description	<i>disable</i>	Disable this interface in the SD-WAN.	<i>enable</i>	Enable this interface in the SD-WAN.
Option	Description									
<i>disable</i>	Disable this interface in the SD-WAN.									
<i>enable</i>	Enable this interface in the SD-WAN.									
comment	Comments.	var-string	Maximum length: 255							

## config neighbor

Parameter	Description	Type	Size	Default
ip	IP/IPv6 address of neighbor.	string	Maximum length: 45	
member	Member sequence number.	integer	Minimum value: 0 Maximum value: 4294967295	0

Parameter	Description	Type	Size	Default
mode	What metric to select the neighbor.	option	-	sla
	<b>Option</b>	<b>Description</b>		
	<i>sla</i>	Select neighbor based on SLA link quality.		
	<i>speedtest</i>	Select neighbor based on the speedtest status.		
role	Role of neighbor.	option	-	standalone
	<b>Option</b>	<b>Description</b>		
	<i>standalone</i>	Standalone neighbor.		
	<i>primary</i>	Primary neighbor.		
	<i>secondary</i>	Secondary neighbor.		
health-check	SD-WAN health-check name.	string	Maximum length: 35	
sla-id	SLA ID.	integer	Minimum value: 0 Maximum value: 4294967295	0

## config service

Parameter	Description	Type	Size	Default
id	SD-WAN rule ID.	integer	Minimum value: 1 Maximum value: 4000	0
name	SD-WAN rule name.	string	Maximum length: 35	
addr-mode	Address mode (IPv4 or IPv6).	option	-	ipv4
	<b>Option</b>	<b>Description</b>		
	<i>ipv4</i>	IPv4 mode.		
	<i>ipv6</i>	IPv6 mode.		
input-device <name>	Source interface name. Interface name.	string	Maximum length: 79	
input-device-negate	Enable/disable negation of input device match.	option	-	disable

Parameter	Description	Type	Size	Default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable negation of input device match.</td></tr><tr><td><i>disable</i></td><td>Disable negation of input device match.</td></tr></table>	Option	Description	<i>enable</i>	Enable negation of input device match.	<i>disable</i>	Disable negation of input device match.											
	Option	Description																
	<i>enable</i>	Enable negation of input device match.																
<i>disable</i>	Disable negation of input device match.																	
mode	Control how the SD-WAN rule sets the priority of interfaces in the SD-WAN.	option	-	manual														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto</i></td><td>Assign interfaces a priority based on quality.</td></tr><tr><td><i>manual</i></td><td>Assign interfaces a priority manually.</td></tr><tr><td><i>priority</i></td><td>Assign interfaces a priority based on the link-cost-factor quality of the interface.</td></tr><tr><td><i>sla</i></td><td>Assign interfaces a priority based on selected SLA settings.</td></tr><tr><td><i>load-balance</i></td><td>Distribute traffic among all available links based on round robin. ADVPN feature is not supported in the mode.</td></tr></table>	Option	Description	<i>auto</i>	Assign interfaces a priority based on quality.	<i>manual</i>	Assign interfaces a priority manually.	<i>priority</i>	Assign interfaces a priority based on the link-cost-factor quality of the interface.	<i>sla</i>	Assign interfaces a priority based on selected SLA settings.	<i>load-balance</i>	Distribute traffic among all available links based on round robin. ADVPN feature is not supported in the mode.					
	Option	Description																
	<i>auto</i>	Assign interfaces a priority based on quality.																
	<i>manual</i>	Assign interfaces a priority manually.																
	<i>priority</i>	Assign interfaces a priority based on the link-cost-factor quality of the interface.																
	<i>sla</i>	Assign interfaces a priority based on selected SLA settings.																
<i>load-balance</i>	Distribute traffic among all available links based on round robin. ADVPN feature is not supported in the mode.																	
minimum-sla-meet-members	Minimum number of members which meet SLA.	integer	Minimum value: 0 Maximum value: 255	0														
hash-mode	Hash algorithm for selected priority members for load balance mode.	option	-	round-robin														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>round-robin</i></td><td>All traffic are distributed to selected interfaces in equal portions and circular order.</td></tr><tr><td><i>source-ip-based</i></td><td>All traffic from a source IP is sent to the same interface.</td></tr><tr><td><i>source-dest-ip-based</i></td><td>All traffic from a source IP to a destination IP is sent to the same interface.</td></tr><tr><td><i>inbandwidth</i></td><td>All traffic are distributed to a selected interface with most available bandwidth for incoming traffic.</td></tr><tr><td><i>outbandwidth</i></td><td>All traffic are distributed to a selected interface with most available bandwidth for outgoing traffic.</td></tr><tr><td><i>bibandwidth</i></td><td>All traffic are distributed to a selected interface with most available bandwidth for both incoming and outgoing traffic.</td></tr></table>	Option	Description	<i>round-robin</i>	All traffic are distributed to selected interfaces in equal portions and circular order.	<i>source-ip-based</i>	All traffic from a source IP is sent to the same interface.	<i>source-dest-ip-based</i>	All traffic from a source IP to a destination IP is sent to the same interface.	<i>inbandwidth</i>	All traffic are distributed to a selected interface with most available bandwidth for incoming traffic.	<i>outbandwidth</i>	All traffic are distributed to a selected interface with most available bandwidth for outgoing traffic.	<i>bibandwidth</i>	All traffic are distributed to a selected interface with most available bandwidth for both incoming and outgoing traffic.			
	Option	Description																
	<i>round-robin</i>	All traffic are distributed to selected interfaces in equal portions and circular order.																
	<i>source-ip-based</i>	All traffic from a source IP is sent to the same interface.																
	<i>source-dest-ip-based</i>	All traffic from a source IP to a destination IP is sent to the same interface.																
	<i>inbandwidth</i>	All traffic are distributed to a selected interface with most available bandwidth for incoming traffic.																
	<i>outbandwidth</i>	All traffic are distributed to a selected interface with most available bandwidth for outgoing traffic.																
<i>bibandwidth</i>	All traffic are distributed to a selected interface with most available bandwidth for both incoming and outgoing traffic.																	
role	Service role to work with neighbor.	option	-	standalone														

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>standalone</i>	Standalone service.		
	<i>primary</i>	Primary service for primary neighbor.		
	<i>secondary</i>	Secondary service for secondary neighbor.		
standalone-action	Enable/disable service when selected neighbor role is standalone while service role is not standalone.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable service when selected neighbor role is standalone.		
	<i>disable</i>	Disable service when selected neighbor role is standalone.		
quality-link	Quality grade.	integer	Minimum value: 0 Maximum value: 255	0
tos	Type of service bit pattern.	user	Not Specified	
tos-mask	Type of service evaluated bits.	user	Not Specified	
protocol	Protocol number.	integer	Minimum value: 0 Maximum value: 255	0
start-port	Start destination port number.	integer	Minimum value: 0 Maximum value: 65535	1
end-port	End destination port number.	integer	Minimum value: 0 Maximum value: 65535	65535
route-tag	IPv4 route map route-tag.	integer	Minimum value: 0 Maximum value: 4294967295	0
dst <name>	Destination address name. Address or address group name.	string	Maximum length: 79	

Parameter	Description	Type	Size	Default						
dst-negate	Enable/disable negation of destination address match.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable destination address negation.</td></tr><tr><td>disable</td><td>Disable destination address negation.</td></tr></table>	Option	Description	enable	Enable destination address negation.	disable	Disable destination address negation.			
Option	Description									
enable	Enable destination address negation.									
disable	Disable destination address negation.									
src <name>	Source address name. Address or address group name.	string	Maximum length: 79							
dst6 <name>	Destination address6 name. Address6 or address6 group name.	string	Maximum length: 79							
src6 <name>	Source address6 name. Address6 or address6 group name.	string	Maximum length: 79							
src-negate	Enable/disable negation of source address match.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable source address negation.</td></tr><tr><td>disable</td><td>Disable source address negation.</td></tr></table>	Option	Description	enable	Enable source address negation.	disable	Disable source address negation.			
Option	Description									
enable	Enable source address negation.									
disable	Disable source address negation.									
users <name>	User name. User name.	string	Maximum length: 79							
groups <name>	User groups. Group name.	string	Maximum length: 79							
internet-service	Enable/disable use of Internet service for application-based load balancing.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable cloud service to support application-based load balancing.</td></tr><tr><td>disable</td><td>Disable cloud service to support application-based load balancing.</td></tr></table>	Option	Description	enable	Enable cloud service to support application-based load balancing.	disable	Disable cloud service to support application-based load balancing.			
Option	Description									
enable	Enable cloud service to support application-based load balancing.									
disable	Disable cloud service to support application-based load balancing.									
internet-service-custom <name>	Custom Internet service name list. Custom Internet service name.	string	Maximum length: 79							
internet-service-custom-group <name>	Custom Internet Service group list. Custom Internet Service group name.	string	Maximum length: 79							
internet-service-name <name>	Internet service name list. Internet service name.	string	Maximum length: 79							
internet-service-group <name>	Internet Service group list. Internet Service group name.	string	Maximum length: 79							



Parameter	Description	Type	Size	Default																
internet-service-app-ctrl <id>	Application control based Internet Service ID list. Application control based Internet Service ID.	integer	Minimum value: 0 Maximum value: 4294967295																	
internet-service-app-ctrl-group <name>	Application control based Internet Service group list. Application control based Internet Service group name.	string	Maximum length: 79																	
health-check <name>	Health check list. Health check name.	string	Maximum length: 79																	
link-cost-factor	Link cost factor.	option	-	latency																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>latency</td><td>Select link based on latency.</td></tr><tr><td>jitter</td><td>Select link based on jitter.</td></tr><tr><td>packet-loss</td><td>Select link based on packet loss.</td></tr><tr><td>inbandwidth</td><td>Select link based on available bandwidth of incoming traffic.</td></tr><tr><td>outbandwidth</td><td>Select link based on available bandwidth of outgoing traffic.</td></tr><tr><td>bibandwidth</td><td>Select link based on available bandwidth of bidirectional traffic.</td></tr><tr><td>custom-profile-1</td><td>Select link based on customized profile.</td></tr></table>				Option	Description	latency	Select link based on latency.	jitter	Select link based on jitter.	packet-loss	Select link based on packet loss.	inbandwidth	Select link based on available bandwidth of incoming traffic.	outbandwidth	Select link based on available bandwidth of outgoing traffic.	bibandwidth	Select link based on available bandwidth of bidirectional traffic.	custom-profile-1	Select link based on customized profile.
Option	Description																			
latency	Select link based on latency.																			
jitter	Select link based on jitter.																			
packet-loss	Select link based on packet loss.																			
inbandwidth	Select link based on available bandwidth of incoming traffic.																			
outbandwidth	Select link based on available bandwidth of outgoing traffic.																			
bibandwidth	Select link based on available bandwidth of bidirectional traffic.																			
custom-profile-1	Select link based on customized profile.																			
packet-loss-weight	Coefficient of packet-loss in the formula of custom-profile-1.	integer	Minimum value: 0 Maximum value: 10000000	0																
latency-weight	Coefficient of latency in the formula of custom-profile-1.	integer	Minimum value: 0 Maximum value: 10000000	0																
jitter-weight	Coefficient of jitter in the formula of custom-profile-1.	integer	Minimum value: 0 Maximum value: 10000000	0																

Parameter	Description	Type	Size	Default
bandwidth-weight	Coefficient of reciprocal of available bidirectional bandwidth in the formula of custom-profile-1.	integer	Minimum value: 0 Maximum value: 10000000	0
link-cost-threshold	Percentage threshold change of link cost values that will result in policy route regeneration.	integer	Minimum value: 0 Maximum value: 10000000	10
hold-down-time	Waiting period in seconds when switching from the back-up member to the primary member.	integer	Minimum value: 0 Maximum value: 10000000	0
dscp-forward	Enable/disable forward traffic DSCP tag.	option	-	disable
	Option	Description		
	enable	Enable use of forward DSCP tag.		
	disable	Disable use of forward DSCP tag.		
dscp-reverse	Enable/disable reverse traffic DSCP tag.	option	-	disable
	Option	Description		
	enable	Enable use of reverse DSCP tag.		
	disable	Disable use of reverse DSCP tag.		
dscp-forward-tag	Forward traffic DSCP tag.	user	Not Specified	
dscp-reverse-tag	Reverse traffic DSCP tag.	user	Not Specified	
priority-members <seq-num>	Member sequence number list. Member sequence number.	integer	Minimum value: 0 Maximum value: 4294967295	
priority-zone <name>	Priority zone name list. Priority zone name.	string	Maximum length: 79	
status	Enable/disable SD-WAN service.	option	-	enable

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable SD-WAN service.		
	<i>disable</i>	Disable SD-WAN service.		
gateway	Enable/disable SD-WAN service gateway.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable SD-WAN service gateway.		
	<i>disable</i>	Disable SD-WAN service gateway.		
default	Enable/disable use of SD-WAN as default service.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable use of SD-WAN as default service.		
	<i>disable</i>	Disable use of SD-WAN as default service.		
sla-compare-method	Method to compare SLA value for SLA mode.	option	-	order
	<b>Option</b>	<b>Description</b>		
	<i>order</i>	Compare SLA value based on the order of health-check.		
	<i>number</i>	Compare SLA value based on the number of satisfied health-check. Limits health-checks to only configured member interfaces.		
tie-break	Method of selecting member if more than one meets the SLA.	option	-	zone
	<b>Option</b>	<b>Description</b>		
	<i>zone</i>	Use the setting that is configured for the members' zone.		
	<i>cfg-order</i>	Members that meet the SLA are selected in the order they are configured.		
	<i>fib-best-match</i>	Members that meet the SLA are selected that match the longest prefix in the routing table.		
use-shortcut-sla	Enable/disable use of ADVPN shortcut for quality comparison.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable use of ADVPN shortcut for quality comparison.		
	<i>disable</i>	Disable use of ADVPN shortcut for quality comparison.		

Parameter	Description	Type	Size	Default
passive-measurement	Enable/disable passive measurement based on the service criteria.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable passive measurement of user traffic.		
	<i>disable</i>	Disable passive measurement of user traffic.		

### config sla

Parameter	Description	Type	Size	Default
health-check	SD-WAN health-check.	string	Maximum length: 35	
id	SLA ID.	integer	Minimum value: 0 Maximum value: 4294967295	0

### config zone

Parameter	Description	Type	Size	Default
name	Zone name.	string	Maximum length: 35	
service-sla-tie-break	Method of selecting member if more than one meets the SLA.	option	-	cfg-order
	<b>Option</b>	<b>Description</b>		
	<i>cfg-order</i>	Members that meet the SLA are selected in the order they are configured.		
	<i>fib-best-match</i>	Members that meet the SLA are selected that match the longest prefix in the routing table.		

## config system session-helper

Configure session helper.

```
config system session-helper
  Description: Configure session helper.
  edit <id>
    set name [ftp|tftp|...]
    set port {integer}
    set protocol {integer}
```

next  
end

## config system session-helper

Parameter	Description	Type	Size	Default																																
id	Session helper ID.	integer	Minimum value: 0 Maximum value: 4294967295	0																																
name	Helper name.	option	-																																	
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ftp</i></td><td>FTP.</td></tr><tr><td><i>tftp</i></td><td>TFTP.</td></tr><tr><td><i>ras</i></td><td>RAS.</td></tr><tr><td><i>h323</i></td><td>H323.</td></tr><tr><td><i>tns</i></td><td>TNS.</td></tr><tr><td><i>mms</i></td><td>MMS.</td></tr><tr><td><i>sip</i></td><td>SIP.</td></tr><tr><td><i>pptp</i></td><td>PPTP.</td></tr><tr><td><i>rtsp</i></td><td>RTSP.</td></tr><tr><td><i>dns-udp</i></td><td>DNS UDP.</td></tr><tr><td><i>dns-tcp</i></td><td>DNS TCP.</td></tr><tr><td><i>pmap</i></td><td>PMAP.</td></tr><tr><td><i>rsh</i></td><td>RSH.</td></tr><tr><td><i>dcerpc</i></td><td>DCERPC.</td></tr><tr><td><i>mgcp</i></td><td>MGCP.</td></tr></table>	Option	Description	<i>ftp</i>	FTP.	<i>tftp</i>	TFTP.	<i>ras</i>	RAS.	<i>h323</i>	H323.	<i>tns</i>	TNS.	<i>mms</i>	MMS.	<i>sip</i>	SIP.	<i>pptp</i>	PPTP.	<i>rtsp</i>	RTSP.	<i>dns-udp</i>	DNS UDP.	<i>dns-tcp</i>	DNS TCP.	<i>pmap</i>	PMAP.	<i>rsh</i>	RSH.	<i>dcerpc</i>	DCERPC.	<i>mgcp</i>	MGCP.			
	Option	Description																																		
	<i>ftp</i>	FTP.																																		
	<i>tftp</i>	TFTP.																																		
	<i>ras</i>	RAS.																																		
	<i>h323</i>	H323.																																		
	<i>tns</i>	TNS.																																		
	<i>mms</i>	MMS.																																		
	<i>sip</i>	SIP.																																		
	<i>pptp</i>	PPTP.																																		
	<i>rtsp</i>	RTSP.																																		
	<i>dns-udp</i>	DNS UDP.																																		
	<i>dns-tcp</i>	DNS TCP.																																		
	<i>pmap</i>	PMAP.																																		
	<i>rsh</i>	RSH.																																		
<i>dcerpc</i>	DCERPC.																																			
<i>mgcp</i>	MGCP.																																			
port	Protocol port.	integer	Minimum value: 1 Maximum value: 65535	0																																
protocol	Protocol number.	integer	Minimum value: 0 Maximum value: 255	0																																

## config system session-ttl

Configure global session TTL timers for this FortiGate.

```
config system session-ttl
  Description: Configure global session TTL timers for this FortiGate.
  set default {user}
  config port
    Description: Session TTL port.
    edit <id>
      set protocol {integer}
      set start-port {integer}
      set end-port {integer}
      set timeout {user}
    next
  end
end
```

## config system session-ttl

Parameter	Description	Type	Size	Default
default	Default timeout.	user	Not Specified	

## config port

Parameter	Description	Type	Size	Default
id	Table entry ID.	integer	Minimum value: 0 Maximum value: 65535	0
protocol	Protocol.	integer	Minimum value: 0 Maximum value: 255	0
start-port	Start port number.	integer	Minimum value: 0 Maximum value: 65535	0
end-port	End port number.	integer	Minimum value: 0 Maximum value: 65535	0

Parameter	Description	Type	Size	Default
timeout	Session timeout (TTL).	user	Not Specified	

## config system settings

Configure VDOM settings.

```
config system settings
    Description: Configure VDOM settings.
    set allow-linkdown-path [enable|disable]
    set allow-subnet-overlap [enable|disable]
    set application-bandwidth-tracking [disable|enable]
    set asymroute [enable|disable]
    set asymroute-icmp [enable|disable]
    set asymroute6 [enable|disable]
    set asymroute6-icmp [enable|disable]
    set auxiliary-session [enable|disable]
    set bfd [enable|disable]
    set bfd-desired-min-tx {integer}
    set bfd-detect-mult {integer}
    set bfd-dont-enforce-src-port [enable|disable]
    set bfd-required-min-rx {integer}
    set block-land-attack [disable|enable]
    set central-nat [enable|disable]
    set comments {var-string}
    set default-voip-alg-mode [proxy-based|kernel-helper-based]
    set deny-tcp-with-icmp [enable|disable]
    set device {string}
    set dhcp-proxy [enable|disable]
    set dhcp-proxy-interface {string}
    set dhcp-proxy-interface-select-method [auto|sdwan|...]
    set dhcp-server-ip {user}
    set dhcp6-server-ip {user}
    set discovered-device-timeout {integer}
    set ecmp-max-paths {integer}
    set email-portal-check-dns [disable|enable]
    set firewall-session-dirty [check-all|check-new|...]
    set fw-session-hairpin [enable|disable]
    set gateway {ipv4-address}
    set gateway6 {ipv6-address}
    set gtp-asym-fgsp [disable|enable]
    set gtp-monitor-mode [enable|disable]
    set gui-advanced-policy [enable|disable]
    set gui-allow-unnamed-policy [enable|disable]
    set gui-antivirus [enable|disable]
    set gui-ap-profile [enable|disable]
    set gui-application-control [enable|disable]
    set gui-default-policy-columns <name1>, <name2>, ...
    set gui-dhcp-advanced [enable|disable]
    set gui-dns-database [enable|disable]
    set gui-dnsfilter [enable|disable]
    set gui-dos-policy [enable|disable]
```

---

```
set gui-dynamic-routing [enable|disable]
set gui-email-collection [enable|disable]
set gui-endpoint-control [enable|disable]
set gui-endpoint-control-advanced [enable|disable]
set gui-explicit-proxy [enable|disable]
set gui-file-filter [enable|disable]
set gui-fortiap-split-tunneling [enable|disable]
set gui-fortitextender-controller [enable|disable]
set gui-icap [enable|disable]
set gui-implicit-policy [enable|disable]
set gui-ips [enable|disable]
set gui-load-balance [enable|disable]
set gui-local-in-policy [enable|disable]
set gui-local-reports [enable|disable]
set gui-multicast-policy [enable|disable]
set gui-multiple-interface-policy [enable|disable]
set gui-object-colors [enable|disable]
set gui-policy-based-ipsec [enable|disable]
set gui-policy-disclaimer [enable|disable]
set gui-security-profile-group [enable|disable]
set gui-spamfilter [enable|disable]
set gui-sslvpn-personal-bookmarks [enable|disable]
set gui-sslvpn-realms [enable|disable]
set gui-switch-controller [enable|disable]
set gui-threat-weight [enable|disable]
set gui-traffic-shaping [enable|disable]
set gui-videofilter [enable|disable]
set gui-voip-profile [enable|disable]
set gui-vpn [enable|disable]
set gui-waf-profile [enable|disable]
set gui-wan-load-balancing [enable|disable]
set gui-wanopt-cache [enable|disable]
set gui-webfilter [enable|disable]
set gui-webfilter-advanced [enable|disable]
set gui-wireless-controller [enable|disable]
set gui-ztna [enable|disable]
set h323-direct-model [disable|enable]
set http-external-dest [fortiweb|forticache]
set hyperscale-default-policy-action [drop-on-hardware|forward-to-host]
set ike-dn-format [with-space|no-space]
set ike-policy-route [enable|disable]
set ike-port {integer}
set ike-quick-crash-detect [enable|disable]
set ike-session-resume [enable|disable]
set ip {ipv4-classnet-host}
set ip6 {ipv6-prefix}
set link-down-access [enable|disable]
set lldp-reception [enable|disable|...]
set lldp-transmission [enable|disable|...]
set location-id {ipv4-address}
set mac-ttl {integer}
set manageip {user}
set manageip6 {ipv6-prefix}
set multicast-forward [enable|disable]
set multicast-skip-policy [enable|disable]
set multicast-ttl-notchange [enable|disable]
```



```

set nat46-force-ipv4-packet-forwarding [enable|disable]
set nat46-generate-ipv6-fragment-header [enable|disable]
set nat64-force-ipv6-packet-forwarding [enable|disable]
set ngfw-mode [profile-based|policy-based]
set opmode [nat|transparent]
set pfcf-monitor-mode [enable|disable]
set policy-offload-level [disable|dos-offload]
set prp-trailer-action [enable|disable]
set sccp-port {integer}
set sctp-session-without-init [enable|disable]
set ses-denied-traffic [enable|disable]
set session-insert-trial [enable|disable]
set sip-expectation [enable|disable]
set sip-nat-trace [enable|disable]
set sip-ssl-port {integer}
set sip-tcp-port {integer}
set sip-udp-port {integer}
set snat-hairpin-traffic [enable|disable]
set status [enable|disable]
set strict-src-check [enable|disable]
set tcp-session-without-syn [enable|disable]
set trap-local-session [disable|enable]
set trap-session-flag [udp-both|udp-reply|...]
set utf8-spam-tagging [enable|disable]
set v4-ecmp-mode [source-ip-based|weight-based|...]
set vpn-stats-log {option1}, {option2}, ...
set vpn-stats-period {integer}
set wccp-cache-engine [enable|disable]

```

end

## config system settings

Parameter	Description	Type	Size	Default						
allow-linkdown-path	Enable/disable link down path.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Allow link down path.</td></tr><tr><td><i>disable</i></td><td>Do not allow link down path.</td></tr></table>	Option	Description	<i>enable</i>	Allow link down path.	<i>disable</i>	Do not allow link down path.			
Option	Description									
<i>enable</i>	Allow link down path.									
<i>disable</i>	Do not allow link down path.									
allow-subnet-overlap	Enable/disable allowing interface subnets to use overlapping IP addresses.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable overlapping subnets.</td></tr><tr><td><i>disable</i></td><td>Disable overlapping subnets.</td></tr></table>	Option	Description	<i>enable</i>	Enable overlapping subnets.	<i>disable</i>	Disable overlapping subnets.			
Option	Description									
<i>enable</i>	Enable overlapping subnets.									
<i>disable</i>	Disable overlapping subnets.									
application-bandwidth-tracking	Enable/disable application bandwidth tracking.	option	-	disable						

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable application bandwidth tracking.		
	<i>enable</i>	Enable application bandwidth tracking.		
asymroute	Enable/disable IPv4 asymmetric routing.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable IPv4 asymmetric routing.		
	<i>disable</i>	Disable IPv4 asymmetric routing.		
asymroute-icmp	Enable/disable ICMP asymmetric routing.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable ICMP asymmetric routing.		
	<i>disable</i>	Disable ICMP asymmetric routing.		
asymroute6	Enable/disable asymmetric IPv6 routing.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable asymmetric IPv6 routing.		
	<i>disable</i>	Disable asymmetric IPv6 routing.		
asymroute6-icmp	Enable/disable asymmetric ICMPv6 routing.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable asymmetric ICMPv6 routing.		
	<i>disable</i>	Disable asymmetric ICMPv6 routing.		
auxiliary-session *	Enable/disable auxiliary session.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable auxiliary session for this VDOM.		
	<i>disable</i>	Disable auxiliary session for this VDOM.		
bfd	Enable/disable Bi-directional Forwarding Detection (BFD) on all interfaces.	option	-	disable

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable Bi-directional Forwarding Detection (BFD) on all interfaces.		
	<i>disable</i>	Disable Bi-directional Forwarding Detection (BFD) on all interfaces.		
bfd-desired-min-tx	BFD desired minimal transmit interval.	integer	Minimum value: 1 Maximum value: 100000	250
bfd-detect-mult	BFD detection multiplier.	integer	Minimum value: 1 Maximum value: 50	3
bfd-dont-enforce-src-port	Enable to not enforce verifying the source port of BFD Packets.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable verifying the source port of BFD Packets.		
	<i>disable</i>	Disable verifying the source port of BFD Packets.		
bfd-required-min-rx	BFD required minimal receive interval.	integer	Minimum value: 1 Maximum value: 100000	250
block-land-attack	Enable/disable blocking of land attacks.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Do not block land attack.		
	<i>enable</i>	Block land attack.		
central-nat	Enable/disable central NAT.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable central NAT.		
	<i>disable</i>	Disable central NAT.		
comments	VDOM comments.	var-string	Maximum length: 255	

Parameter	Description	Type	Size	Default								
default-voip-alg-mode	Configure how the FortiGate handles VoIP traffic when a policy that accepts the traffic doesn't include a VoIP profile.	option	-	proxy-based								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>proxy-based</i></td><td>Use a default proxy-based VoIP ALG.</td></tr><tr><td><i>kernel-helper-based</i></td><td>Use the SIP session helper.</td></tr></table>	Option	Description	<i>proxy-based</i>	Use a default proxy-based VoIP ALG.	<i>kernel-helper-based</i>	Use the SIP session helper.					
Option	Description											
<i>proxy-based</i>	Use a default proxy-based VoIP ALG.											
<i>kernel-helper-based</i>	Use the SIP session helper.											
deny-tcp-with-icmp	Enable/disable denying TCP by sending an ICMP communication prohibited packet.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Deny TCP with ICMP.</td></tr><tr><td><i>disable</i></td><td>Disable denying TCP with ICMP.</td></tr></table>	Option	Description	<i>enable</i>	Deny TCP with ICMP.	<i>disable</i>	Disable denying TCP with ICMP.					
Option	Description											
<i>enable</i>	Deny TCP with ICMP.											
<i>disable</i>	Disable denying TCP with ICMP.											
device	Interface to use for management access for NAT mode.	string	Maximum length: 35									
dhcp-proxy	Enable/disable the DHCP Proxy.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable the DHCP proxy.</td></tr><tr><td><i>disable</i></td><td>Disable the DHCP proxy.</td></tr></table>	Option	Description	<i>enable</i>	Enable the DHCP proxy.	<i>disable</i>	Disable the DHCP proxy.					
Option	Description											
<i>enable</i>	Enable the DHCP proxy.											
<i>disable</i>	Disable the DHCP proxy.											
dhcp-proxy-interface	Specify outgoing interface to reach server.	string	Maximum length: 15									
dhcp-proxy-interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto</i></td><td>Set outgoing interface automatically.</td></tr><tr><td><i>sdwan</i></td><td>Set outgoing interface by SD-WAN or policy routing rules.</td></tr><tr><td><i>specify</i></td><td>Set outgoing interface manually.</td></tr></table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.			
Option	Description											
<i>auto</i>	Set outgoing interface automatically.											
<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.											
<i>specify</i>	Set outgoing interface manually.											
dhcp-server-ip	DHCP Server IPv4 address.	user	Not Specified									
dhcp6-server-ip	DHCPv6 server IPv6 address.	user	Not Specified									

Parameter	Description	Type	Size	Default
discovered-device-timeout	Timeout for discovered devices.	integer	Minimum value: 1 Maximum value: 365	28
ecmp-max-paths	Maximum number of Equal Cost Multi-Path.	integer	Minimum value: 1 Maximum value: 255	255
email-portal-check-dns	Enable/disable using DNS to validate email addresses collected by a captive portal.	option	-	enable
	<b>Option</b>		<b>Description</b>	
	<i>disable</i>		Disable email address checking with DNS.	
	<i>enable</i>		Enable email address checking with DNS.	
firewall-session-dirty	Select how to manage sessions affected by firewall policy configuration changes.	option	-	check-all
	<b>Option</b>		<b>Description</b>	
	<i>check-all</i>		All sessions affected by a firewall policy change are flushed from the session table. When new packets are received they are re-evaluated by stateful inspection and re-added to the session table.	
	<i>check-new</i>		Established sessions for changed firewall policies continue without being affected by the policy configuration change. New sessions are evaluated according to the new firewall policy configuration.	
	<i>check-policy-option</i>		Sessions are managed individually depending on the firewall policy. Some sessions may restart. Some may continue.	
fw-session-hairpin	Enable/disable checking for a matching policy each time hairpin traffic goes through the FortiGate.	option	-	disable
	<b>Option</b>		<b>Description</b>	
	<i>enable</i>		Perform a policy check every time.	
	<i>disable</i>		Perform a policy check only the first time the session is received.	
gateway	Transparent mode IPv4 default gateway IP address.	ipv4-address	Not Specified	0.0.0.0
gateway6	Transparent mode IPv6 default gateway IP address.	ipv6-address	Not Specified	::
gtp-asym-fgsp *	Enable/disable GTP asymmetric traffic handling on FGSP.	option	-	disable

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable GTP asymmetric traffic handling on FGSP.		
	<i>enable</i>	Enable GTP asymmetric traffic handling on FGSP.		
gtp-monitor-mode *	Enable/disable GTP monitor mode (VDOM level).	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable GTP monitor mode.		
	<i>disable</i>	Disable GTP monitor mode.		
gui-advanced-policy	Enable/disable advanced policy configuration on the GUI.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable advanced policy configuration on the GUI.		
	<i>disable</i>	Disable advanced policy configuration on the GUI.		
gui-allow-unnamed-policy	Enable/disable the requirement for policy naming on the GUI.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable the requirement for policy naming on the GUI.		
	<i>disable</i>	Disable the requirement for policy naming on the GUI.		
gui-antivirus	Enable/disable AntiVirus on the GUI.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable AntiVirus on the GUI.		
	<i>disable</i>	Disable AntiVirus on the GUI.		
gui-ap-profile	Enable/disable FortiAP profiles on the GUI.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable FortiAP profiles on the GUI.		
	<i>disable</i>	Disable FortiAP profiles on the GUI.		
gui-application-control	Enable/disable application control on the GUI.	option	-	enable

Parameter	Description	Type	Size	Default
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Enable application control on the GUI.		
	<i>disable</i>	Disable application control on the GUI.		
gui-default-policy-columns <name>	Default columns to display for policy lists on GUI. Select column name.	string	Maximum length: 79	
gui-dhcp-advanced	Enable/disable advanced DHCP options on the GUI.	option	-	enable
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Enable advanced DHCP options on the GUI.		
	<i>disable</i>	Disable advanced DHCP options on the GUI.		
gui-dns-database	Enable/disable DNS database settings on the GUI.	option	-	disable
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Enable DNS database settings on the GUI.		
	<i>disable</i>	Disable DNS database settings on the GUI.		
gui-dnsfilter	Enable/disable DNS Filtering on the GUI.	option	-	enable **
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Enable DNS Filtering on the GUI.		
	<i>disable</i>	Disable DNS Filtering on the GUI.		
gui-dos-policy	Enable/disable DoS policies on the GUI.	option	-	enable **
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Enable DoS policies on the GUI.		
	<i>disable</i>	Disable DoS policies on the GUI.		
gui-dynamic-routing	Enable/disable dynamic routing on the GUI.	option	-	enable **
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Enable dynamic routing on the GUI.		
	<i>disable</i>	Disable dynamic routing on the GUI.		

Parameter	Description	Type	Size	Default						
gui-email-collection	Enable/disable email collection on the GUI.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable email collection on the GUI.</td></tr><tr><td><i>disable</i></td><td>Disable email collection on the GUI.</td></tr></table>	Option	Description	<i>enable</i>	Enable email collection on the GUI.	<i>disable</i>	Disable email collection on the GUI.			
Option	Description									
<i>enable</i>	Enable email collection on the GUI.									
<i>disable</i>	Disable email collection on the GUI.									
gui-endpoint-control	Enable/disable endpoint control on the GUI.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable endpoint control on the GUI.</td></tr><tr><td><i>disable</i></td><td>Disable endpoint control on the GUI.</td></tr></table>	Option	Description	<i>enable</i>	Enable endpoint control on the GUI.	<i>disable</i>	Disable endpoint control on the GUI.			
Option	Description									
<i>enable</i>	Enable endpoint control on the GUI.									
<i>disable</i>	Disable endpoint control on the GUI.									
gui-endpoint-control-advanced	Enable/disable advanced endpoint control options on the GUI.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable advanced endpoint control options on the GUI.</td></tr><tr><td><i>disable</i></td><td>Disable advanced endpoint control options on the GUI.</td></tr></table>	Option	Description	<i>enable</i>	Enable advanced endpoint control options on the GUI.	<i>disable</i>	Disable advanced endpoint control options on the GUI.			
Option	Description									
<i>enable</i>	Enable advanced endpoint control options on the GUI.									
<i>disable</i>	Disable advanced endpoint control options on the GUI.									
gui-explicit-proxy	Enable/disable the explicit proxy on the GUI.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable the explicit proxy on the GUI.</td></tr><tr><td><i>disable</i></td><td>Disable the explicit proxy on the GUI.</td></tr></table>	Option	Description	<i>enable</i>	Enable the explicit proxy on the GUI.	<i>disable</i>	Disable the explicit proxy on the GUI.			
Option	Description									
<i>enable</i>	Enable the explicit proxy on the GUI.									
<i>disable</i>	Disable the explicit proxy on the GUI.									
gui-file-filter	Enable/disable File-filter on the GUI.	option	-	enable **						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable File-filter on the GUI.</td></tr><tr><td><i>disable</i></td><td>Disable File-filter on the GUI.</td></tr></table>	Option	Description	<i>enable</i>	Enable File-filter on the GUI.	<i>disable</i>	Disable File-filter on the GUI.			
Option	Description									
<i>enable</i>	Enable File-filter on the GUI.									
<i>disable</i>	Disable File-filter on the GUI.									
gui-fortiap-split-tunneling	Enable/disable FortiAP split tunneling on the GUI.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable FortiAP split tunneling on the GUI.</td></tr><tr><td><i>disable</i></td><td>Disable FortiAP split tunneling on the GUI.</td></tr></table>	Option	Description	<i>enable</i>	Enable FortiAP split tunneling on the GUI.	<i>disable</i>	Disable FortiAP split tunneling on the GUI.			
Option	Description									
<i>enable</i>	Enable FortiAP split tunneling on the GUI.									
<i>disable</i>	Disable FortiAP split tunneling on the GUI.									



Parameter	Description	Type	Size	Default						
gui-fortiextender-controller	Enable/disable FortiExtender on the GUI.	option	-	disable **						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable FortiExtender on the GUI.</td></tr><tr><td>disable</td><td>Disable FortiExtender on the GUI.</td></tr></table>	Option	Description	enable	Enable FortiExtender on the GUI.	disable	Disable FortiExtender on the GUI.			
Option	Description									
enable	Enable FortiExtender on the GUI.									
disable	Disable FortiExtender on the GUI.									
gui-icap	Enable/disable ICAP on the GUI.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable ICAP on the GUI.</td></tr><tr><td>disable</td><td>Disable ICAP on the GUI.</td></tr></table>	Option	Description	enable	Enable ICAP on the GUI.	disable	Disable ICAP on the GUI.			
Option	Description									
enable	Enable ICAP on the GUI.									
disable	Disable ICAP on the GUI.									
gui-implicit-policy	Enable/disable implicit firewall policies on the GUI.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable implicit firewall policies on the GUI.</td></tr><tr><td>disable</td><td>Disable implicit firewall policies on the GUI.</td></tr></table>	Option	Description	enable	Enable implicit firewall policies on the GUI.	disable	Disable implicit firewall policies on the GUI.			
Option	Description									
enable	Enable implicit firewall policies on the GUI.									
disable	Disable implicit firewall policies on the GUI.									
gui-ips	Enable/disable IPS on the GUI.	option	-	enable **						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable IPS on the GUI.</td></tr><tr><td>disable</td><td>Disable IPS on the GUI.</td></tr></table>	Option	Description	enable	Enable IPS on the GUI.	disable	Disable IPS on the GUI.			
Option	Description									
enable	Enable IPS on the GUI.									
disable	Disable IPS on the GUI.									
gui-load-balance	Enable/disable server load balancing on the GUI.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable server load balancing on the GUI.</td></tr><tr><td>disable</td><td>Disable server load balancing on the GUI.</td></tr></table>	Option	Description	enable	Enable server load balancing on the GUI.	disable	Disable server load balancing on the GUI.			
Option	Description									
enable	Enable server load balancing on the GUI.									
disable	Disable server load balancing on the GUI.									
gui-local-in-policy	Enable/disable Local-In policies on the GUI.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable Local-In policies on the GUI.</td></tr><tr><td>disable</td><td>Disable Local-In policies on the GUI.</td></tr></table>	Option	Description	enable	Enable Local-In policies on the GUI.	disable	Disable Local-In policies on the GUI.			
Option	Description									
enable	Enable Local-In policies on the GUI.									
disable	Disable Local-In policies on the GUI.									

Parameter	Description	Type	Size	Default						
gui-local-reports *	Enable/disable local reports on the GUI.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable local reports on the GUI.</td></tr><tr><td><i>disable</i></td><td>Disable local reports on the GUI.</td></tr></table>	Option	Description	<i>enable</i>	Enable local reports on the GUI.	<i>disable</i>	Disable local reports on the GUI.			
Option	Description									
<i>enable</i>	Enable local reports on the GUI.									
<i>disable</i>	Disable local reports on the GUI.									
gui-multicast-policy	Enable/disable multicast firewall policies on the GUI.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable multicast firewall policies on the GUI.</td></tr><tr><td><i>disable</i></td><td>Disable multicast firewall policies on the GUI.</td></tr></table>	Option	Description	<i>enable</i>	Enable multicast firewall policies on the GUI.	<i>disable</i>	Disable multicast firewall policies on the GUI.			
Option	Description									
<i>enable</i>	Enable multicast firewall policies on the GUI.									
<i>disable</i>	Disable multicast firewall policies on the GUI.									
gui-multiple-interface-policy	Enable/disable adding multiple interfaces to a policy on the GUI.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable adding multiple interfaces to a policy on the GUI.</td></tr><tr><td><i>disable</i></td><td>Disable adding multiple interfaces to a policy on the GUI.</td></tr></table>	Option	Description	<i>enable</i>	Enable adding multiple interfaces to a policy on the GUI.	<i>disable</i>	Disable adding multiple interfaces to a policy on the GUI.			
Option	Description									
<i>enable</i>	Enable adding multiple interfaces to a policy on the GUI.									
<i>disable</i>	Disable adding multiple interfaces to a policy on the GUI.									
gui-object-colors	Enable/disable object colors on the GUI.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable object colors on the GUI.</td></tr><tr><td><i>disable</i></td><td>Disable object colors on the GUI.</td></tr></table>	Option	Description	<i>enable</i>	Enable object colors on the GUI.	<i>disable</i>	Disable object colors on the GUI.			
Option	Description									
<i>enable</i>	Enable object colors on the GUI.									
<i>disable</i>	Disable object colors on the GUI.									
gui-policy-based-ipsec	Enable/disable policy-based IPsec VPN on the GUI.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable policy-based IPsec VPN on the GUI.</td></tr><tr><td><i>disable</i></td><td>Disable policy-based IPsec VPN on the GUI.</td></tr></table>	Option	Description	<i>enable</i>	Enable policy-based IPsec VPN on the GUI.	<i>disable</i>	Disable policy-based IPsec VPN on the GUI.			
Option	Description									
<i>enable</i>	Enable policy-based IPsec VPN on the GUI.									
<i>disable</i>	Disable policy-based IPsec VPN on the GUI.									
gui-policy-disclaimer	Enable/disable policy disclaimer on the GUI.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable policy disclaimer on the GUI.</td></tr><tr><td><i>disable</i></td><td>Disable policy disclaimer on the GUI.</td></tr></table>	Option	Description	<i>enable</i>	Enable policy disclaimer on the GUI.	<i>disable</i>	Disable policy disclaimer on the GUI.			
Option	Description									
<i>enable</i>	Enable policy disclaimer on the GUI.									
<i>disable</i>	Disable policy disclaimer on the GUI.									

Parameter	Description	Type	Size	Default						
gui-security-profile-group	Enable/disable Security Profile Groups on the GUI.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Security Profile Groups on the GUI.</td></tr><tr><td><i>disable</i></td><td>Disable Security Profile Groups on the GUI.</td></tr></table>	Option	Description	<i>enable</i>	Enable Security Profile Groups on the GUI.	<i>disable</i>	Disable Security Profile Groups on the GUI.			
Option	Description									
<i>enable</i>	Enable Security Profile Groups on the GUI.									
<i>disable</i>	Disable Security Profile Groups on the GUI.									
gui-spamfilter	Enable/disable Antispam on the GUI.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Antispam on the GUI.</td></tr><tr><td><i>disable</i></td><td>Disable Antispam on the GUI.</td></tr></table>	Option	Description	<i>enable</i>	Enable Antispam on the GUI.	<i>disable</i>	Disable Antispam on the GUI.			
Option	Description									
<i>enable</i>	Enable Antispam on the GUI.									
<i>disable</i>	Disable Antispam on the GUI.									
gui-sslvpn-personal-bookmarks	Enable/disable SSL-VPN personal bookmark management on the GUI.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable SSL-VPN personal bookmark management on the GUI.</td></tr><tr><td><i>disable</i></td><td>Disable SSL-VPN personal bookmark management on the GUI.</td></tr></table>	Option	Description	<i>enable</i>	Enable SSL-VPN personal bookmark management on the GUI.	<i>disable</i>	Disable SSL-VPN personal bookmark management on the GUI.			
Option	Description									
<i>enable</i>	Enable SSL-VPN personal bookmark management on the GUI.									
<i>disable</i>	Disable SSL-VPN personal bookmark management on the GUI.									
gui-sslvpn-realms	Enable/disable SSL-VPN realms on the GUI.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable SSL-VPN realms on the GUI.</td></tr><tr><td><i>disable</i></td><td>Disable SSL-VPN realms on the GUI.</td></tr></table>	Option	Description	<i>enable</i>	Enable SSL-VPN realms on the GUI.	<i>disable</i>	Disable SSL-VPN realms on the GUI.			
Option	Description									
<i>enable</i>	Enable SSL-VPN realms on the GUI.									
<i>disable</i>	Disable SSL-VPN realms on the GUI.									
gui-switch-controller *	Enable/disable the switch controller on the GUI.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable the switch controller on the GUI.</td></tr><tr><td><i>disable</i></td><td>Disable the switch controller on the GUI.</td></tr></table>	Option	Description	<i>enable</i>	Enable the switch controller on the GUI.	<i>disable</i>	Disable the switch controller on the GUI.			
Option	Description									
<i>enable</i>	Enable the switch controller on the GUI.									
<i>disable</i>	Disable the switch controller on the GUI.									
gui-threat-weight	Enable/disable threat weight on the GUI.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable threat weight on the GUI.</td></tr><tr><td><i>disable</i></td><td>Disable threat weight on the GUI.</td></tr></table>	Option	Description	<i>enable</i>	Enable threat weight on the GUI.	<i>disable</i>	Disable threat weight on the GUI.			
Option	Description									
<i>enable</i>	Enable threat weight on the GUI.									
<i>disable</i>	Disable threat weight on the GUI.									

Parameter	Description	Type	Size	Default						
gui-traffic-shaping	Enable/disable traffic shaping on the GUI.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable traffic shaping on the GUI.</td></tr><tr><td><i>disable</i></td><td>Disable traffic shaping on the GUI.</td></tr></table>	Option	Description	<i>enable</i>	Enable traffic shaping on the GUI.	<i>disable</i>	Disable traffic shaping on the GUI.			
Option	Description									
<i>enable</i>	Enable traffic shaping on the GUI.									
<i>disable</i>	Disable traffic shaping on the GUI.									
gui-videofilter	Enable/disable Video filtering on the GUI.	option	-	enable **						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Video filtering on the GUI.</td></tr><tr><td><i>disable</i></td><td>Disable Video filtering on the GUI.</td></tr></table>	Option	Description	<i>enable</i>	Enable Video filtering on the GUI.	<i>disable</i>	Disable Video filtering on the GUI.			
Option	Description									
<i>enable</i>	Enable Video filtering on the GUI.									
<i>disable</i>	Disable Video filtering on the GUI.									
gui-voip-profile	Enable/disable VoIP profiles on the GUI.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable VoIP profiles on the GUI.</td></tr><tr><td><i>disable</i></td><td>Disable VoIP profiles on the GUI.</td></tr></table>	Option	Description	<i>enable</i>	Enable VoIP profiles on the GUI.	<i>disable</i>	Disable VoIP profiles on the GUI.			
Option	Description									
<i>enable</i>	Enable VoIP profiles on the GUI.									
<i>disable</i>	Disable VoIP profiles on the GUI.									
gui-vpn	Enable/disable VPN tunnels on the GUI.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable VPN tunnels on the GUI.</td></tr><tr><td><i>disable</i></td><td>Disable VPN tunnels on the GUI.</td></tr></table>	Option	Description	<i>enable</i>	Enable VPN tunnels on the GUI.	<i>disable</i>	Disable VPN tunnels on the GUI.			
Option	Description									
<i>enable</i>	Enable VPN tunnels on the GUI.									
<i>disable</i>	Disable VPN tunnels on the GUI.									
gui-waf-profile	Enable/disable Web Application Firewall on the GUI.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Web Application Firewall on the GUI.</td></tr><tr><td><i>disable</i></td><td>Disable Web Application Firewall on the GUI.</td></tr></table>	Option	Description	<i>enable</i>	Enable Web Application Firewall on the GUI.	<i>disable</i>	Disable Web Application Firewall on the GUI.			
Option	Description									
<i>enable</i>	Enable Web Application Firewall on the GUI.									
<i>disable</i>	Disable Web Application Firewall on the GUI.									
gui-wan-load-balancing	Enable/disable SD-WAN on the GUI.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable SD-WAN on the GUI.</td></tr><tr><td><i>disable</i></td><td>Disable SD-WAN on the GUI.</td></tr></table>	Option	Description	<i>enable</i>	Enable SD-WAN on the GUI.	<i>disable</i>	Disable SD-WAN on the GUI.			
Option	Description									
<i>enable</i>	Enable SD-WAN on the GUI.									
<i>disable</i>	Disable SD-WAN on the GUI.									
gui-wanopt-cache *	Enable/disable WAN Optimization and Web Caching on the GUI.	option	-	disable						

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable WAN Optimization and Web Caching on the GUI.		
	<i>disable</i>	Disable WAN Optimization and Web Caching on the GUI.		
gui-webfilter	Enable/disable Web filtering on the GUI.	option	-	enable **
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable Web filtering on the GUI.		
	<i>disable</i>	Disable Web filtering on the GUI.		
gui-webfilter-advanced	Enable/disable advanced web filtering on the GUI.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable advanced web filtering on the GUI.		
	<i>disable</i>	Disable advanced web filtering on the GUI.		
gui-wireless-controller	Enable/disable the wireless controller on the GUI.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable the wireless controller on the GUI.		
	<i>disable</i>	Disable the wireless controller on the GUI.		
gui-ztna	Enable/disable Zero Trust Network Access features on the GUI.	option	-	enable **
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable Zero Trust Network Access features on the GUI.		
	<i>disable</i>	Disable Zero Trust Network Access features on the GUI.		
h323-direct-model	Enable/disable H323 direct model.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable H323 direct model.		
	<i>enable</i>	Enable H323 direct model.		
http-external-dest	Offload HTTP traffic to FortiWeb or FortiCache.	option	-	fortiweb

Parameter	Description	Type	Size	Default
	<b>Option</b> <b>Description</b>			
	<i>fortiweb</i>	Offload HTTP traffic to FortiWeb for Web Application Firewall inspection.		
	<i>forticache</i>	Offload HTTP traffic to FortiCache for external web caching and WAN optimization.		
hyperscale-default-policy-action *	Hyperscale default policy action.	option	-	drop-on-hardware
	<b>Option</b> <b>Description</b>			
	<i>drop-on-hardware</i>	Drop the packet on hardware.		
	<i>forward-to-host</i>	Forward the packet to cpu.		
ike-dn-format	Configure IKE ASN.1 Distinguished Name format conventions.	option	-	with-space
	<b>Option</b> <b>Description</b>			
	<i>with-space</i>	Format IKE ASN.1 Distinguished Names with spaces between attribute names and values.		
	<i>no-space</i>	Format IKE ASN.1 Distinguished Names without spaces between attribute names and values.		
ike-policy-route	Enable/disable IKE Policy Based Routing (PBR).	option	-	disable
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Enable IKE Policy Based Routing (PBR).		
	<i>disable</i>	Disable IKE Policy Based Routing (PBR).		
ike-port	UDP port for IKE/IPsec traffic.	integer	Minimum value: 1024 Maximum value: 65535	500
ike-quick-crash-detect	Enable/disable IKE quick crash detection (RFC 6290).	option	-	disable
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Enable IKE quick crash detection (RFC 6290).		
	<i>disable</i>	Disable IKE quick crash detection (RFC 6290).		

Parameter	Description	Type	Size	Default								
ike-session-resume	Enable/disable IKEv2 session resumption (RFC 5723).	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable IKEv2 session resumption (RFC 5723).</td></tr><tr><td><i>disable</i></td><td>Disable IKEv2 session resumption (RFC 5723).</td></tr></table>	Option	Description	<i>enable</i>	Enable IKEv2 session resumption (RFC 5723).	<i>disable</i>	Disable IKEv2 session resumption (RFC 5723).					
Option	Description											
<i>enable</i>	Enable IKEv2 session resumption (RFC 5723).											
<i>disable</i>	Disable IKEv2 session resumption (RFC 5723).											
ip	IP address and netmask.	ipv4-classnet-host	Not Specified	0.0.0.0 0.0.0.0								
ip6	IPv6 address prefix for NAT mode.	ipv6-prefix	Not Specified	::/0								
link-down-access	Enable/disable link down access traffic.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Allow link down access traffic.</td></tr><tr><td><i>disable</i></td><td>Block link down access traffic.</td></tr></table>	Option	Description	<i>enable</i>	Allow link down access traffic.	<i>disable</i>	Block link down access traffic.					
Option	Description											
<i>enable</i>	Allow link down access traffic.											
<i>disable</i>	Block link down access traffic.											
lldp-reception	Enable/disable Link Layer Discovery Protocol (LLDP) reception for this VDOM or apply global settings to this VDOM.	option	-	global								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable LLDP reception for this VDOM.</td></tr><tr><td><i>disable</i></td><td>Disable LLDP reception for this VDOM.</td></tr><tr><td><i>global</i></td><td>Use the global LLDP reception configuration for this VDOM.</td></tr></table>	Option	Description	<i>enable</i>	Enable LLDP reception for this VDOM.	<i>disable</i>	Disable LLDP reception for this VDOM.	<i>global</i>	Use the global LLDP reception configuration for this VDOM.			
Option	Description											
<i>enable</i>	Enable LLDP reception for this VDOM.											
<i>disable</i>	Disable LLDP reception for this VDOM.											
<i>global</i>	Use the global LLDP reception configuration for this VDOM.											
lldp-transmission	Enable/disable Link Layer Discovery Protocol (LLDP) transmission for this VDOM or apply global settings to this VDOM.	option	-	global								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable LLDP transmission for this VDOM.</td></tr><tr><td><i>disable</i></td><td>Disable LLDP transmission for this VDOM.</td></tr><tr><td><i>global</i></td><td>Use the global LLDP transmission configuration for this VDOM.</td></tr></table>	Option	Description	<i>enable</i>	Enable LLDP transmission for this VDOM.	<i>disable</i>	Disable LLDP transmission for this VDOM.	<i>global</i>	Use the global LLDP transmission configuration for this VDOM.			
Option	Description											
<i>enable</i>	Enable LLDP transmission for this VDOM.											
<i>disable</i>	Disable LLDP transmission for this VDOM.											
<i>global</i>	Use the global LLDP transmission configuration for this VDOM.											
location-id	Local location ID in the form of an IPv4 address.	ipv4-address	Not Specified	0.0.0.0								

Parameter	Description	Type	Size	Default						
mac-ttl	Duration of MAC addresses in Transparent mode.	integer	Minimum value: 300 Maximum value: 8640000	300						
manageip	Transparent mode IPv4 management IP address and netmask.	user	Not Specified							
manageip6	Transparent mode IPv6 management IP address and netmask.	ipv6-prefix	Not Specified	::/0						
multicast-forward	Enable/disable multicast forwarding.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable multicast forwarding.</td></tr><tr><td>disable</td><td>Disable multicast forwarding.</td></tr></table>	Option	Description	enable	Enable multicast forwarding.	disable	Disable multicast forwarding.			
Option	Description									
enable	Enable multicast forwarding.									
disable	Disable multicast forwarding.									
multicast-skip-policy	Enable/disable allowing multicast traffic through the FortiGate without a policy check.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Allowing multicast traffic through the FortiGate without creating a multicast firewall policy.</td></tr><tr><td>disable</td><td>Require a multicast policy to allow multicast traffic to pass through the FortiGate.</td></tr></table>	Option	Description	enable	Allowing multicast traffic through the FortiGate without creating a multicast firewall policy.	disable	Require a multicast policy to allow multicast traffic to pass through the FortiGate.			
Option	Description									
enable	Allowing multicast traffic through the FortiGate without creating a multicast firewall policy.									
disable	Require a multicast policy to allow multicast traffic to pass through the FortiGate.									
multicast-ttl-notchange	Enable/disable preventing the FortiGate from changing the TTL for forwarded multicast packets.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>The multicast TTL is not changed.</td></tr><tr><td>disable</td><td>The multicast TTL may be changed.</td></tr></table>	Option	Description	enable	The multicast TTL is not changed.	disable	The multicast TTL may be changed.			
Option	Description									
enable	The multicast TTL is not changed.									
disable	The multicast TTL may be changed.									
nat46-force-ipv4-packet-forwarding	Enable/disable mandatory IPv4 packet forwarding in NAT46.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable mandatory IPv4 packet forwarding when IPv4 DF is set to 1.</td></tr><tr><td>disable</td><td>Disable mandatory IPv4 packet forwarding when IPv4 DF is set to 1.</td></tr></table>	Option	Description	enable	Enable mandatory IPv4 packet forwarding when IPv4 DF is set to 1.	disable	Disable mandatory IPv4 packet forwarding when IPv4 DF is set to 1.			
Option	Description									
enable	Enable mandatory IPv4 packet forwarding when IPv4 DF is set to 1.									
disable	Disable mandatory IPv4 packet forwarding when IPv4 DF is set to 1.									



Parameter	Description	Type	Size	Default						
nat46-generate-ipv6-fragment-header	Enable/disable NAT46 IPv6 fragment header generation.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable NAT46 IPv6 fragment header generation.</td></tr><tr><td><i>disable</i></td><td>Disable NAT46 IPv6 fragment header generation.</td></tr></table>	Option	Description	<i>enable</i>	Enable NAT46 IPv6 fragment header generation.	<i>disable</i>	Disable NAT46 IPv6 fragment header generation.			
Option	Description									
<i>enable</i>	Enable NAT46 IPv6 fragment header generation.									
<i>disable</i>	Disable NAT46 IPv6 fragment header generation.									
nat64-force-ipv6-packet-forwarding	Enable/disable mandatory IPv6 packet forwarding in NAT64.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable mandatory IPv6 packet forwarding</td></tr><tr><td><i>disable</i></td><td>Disable mandatory IPv6 packet forwarding</td></tr></table>	Option	Description	<i>enable</i>	Enable mandatory IPv6 packet forwarding	<i>disable</i>	Disable mandatory IPv6 packet forwarding			
Option	Description									
<i>enable</i>	Enable mandatory IPv6 packet forwarding									
<i>disable</i>	Disable mandatory IPv6 packet forwarding									
ngfw-mode	Next Generation Firewall (NGFW) mode.	option	-	profile-based						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>profile-based</i></td><td>Application and web-filtering are configured using profiles applied to policy entries.</td></tr><tr><td><i>policy-based</i></td><td>Application and web-filtering are configured as policy match conditions.</td></tr></table>	Option	Description	<i>profile-based</i>	Application and web-filtering are configured using profiles applied to policy entries.	<i>policy-based</i>	Application and web-filtering are configured as policy match conditions.			
Option	Description									
<i>profile-based</i>	Application and web-filtering are configured using profiles applied to policy entries.									
<i>policy-based</i>	Application and web-filtering are configured as policy match conditions.									
opmode	Firewall operation mode (NAT or Transparent).	option	-	nat						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>nat</i></td><td>Change to NAT mode.</td></tr><tr><td><i>transparent</i></td><td>Change to transparent mode.</td></tr></table>	Option	Description	<i>nat</i>	Change to NAT mode.	<i>transparent</i>	Change to transparent mode.			
Option	Description									
<i>nat</i>	Change to NAT mode.									
<i>transparent</i>	Change to transparent mode.									
pfcf-monitor-mode *	Enable/disable PFCP monitor mode (VDOM level).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable PFCP monitor mode.</td></tr><tr><td><i>disable</i></td><td>Disable PFCP monitor mode.</td></tr></table>	Option	Description	<i>enable</i>	Enable PFCP monitor mode.	<i>disable</i>	Disable PFCP monitor mode.			
Option	Description									
<i>enable</i>	Enable PFCP monitor mode.									
<i>disable</i>	Disable PFCP monitor mode.									
policy-offload-level *	Configure firewall policy offload level.	option	-	disable						

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable policy offloading.		
	<i>dos-offload</i>	Only enable DoS policy offloading.		
prp-trailer-action	Enable/disable action to take on PRP trailer.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Try to keep PRP trailer.		
	<i>disable</i>	Trim PRP trailer.		
sccp-port	TCP port the SCCP proxy monitors for SCCP traffic.	integer	Minimum value: 0 Maximum value: 65535	2000
sctp-session-without-init	Enable/disable Sctp session creation without Sctp INIT.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable Sctp session creation without Sctp INIT.		
	<i>disable</i>	Disable Sctp session creation without Sctp INIT.		
ses-denied-traffic	Enable/disable including denied session in the session table.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Include denied sessions in the session table.		
	<i>disable</i>	Do not add denied sessions to the session table.		
session-insert-trial *	Trial session insert.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable session insert trial/confirm.		
	<i>disable</i>	Disable session insert trial/confirm.		
sip-expectation	Enable/disable the SIP kernel session helper to create an expectation for port 5060.	option	-	disable

Parameter	Description	Type	Size	Default
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Allow SIP session helper to create an expectation for port 5060.		
	<i>disable</i>	Prevent SIP session helper from creating an expectation for port 5060.		
sip-nat-trace	Enable/disable recording the original SIP source IP address when NAT is used.	option	-	enable
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Record the original SIP source IP address when NAT is used.		
	<i>disable</i>	Do not record the original SIP source IP address when NAT is used.		
sip-ssl-port *	TCP port the SIP proxy monitors for SIP SSL/TLS traffic.	integer	Minimum value: 0 Maximum value: 65535	5061
sip-tcp-port	TCP port the SIP proxy monitors for SIP traffic.	integer	Minimum value: 1 Maximum value: 65535	5060
sip-udp-port	UDP port the SIP proxy monitors for SIP traffic.	integer	Minimum value: 1 Maximum value: 65535	5060
snat-hairpin-traffic	Enable/disable source NAT (SNAT) for hairpin traffic.	option	-	enable
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Enable SNAT for hairpin traffic.		
	<i>disable</i>	Disable SNAT for hairpin traffic.		
status	Enable/disable this VDOM.	option	-	enable
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Enable this VDOM.		
	<i>disable</i>	Disable this VDOM.		
strict-src-check	Enable/disable strict source verification.	option	-	disable
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Enable strict source verification.		

Parameter	Description	Type	Size	Default
	<b>Option</b> <b>Description</b>			
	<i>disable</i>			Disable strict source verification.
tcp-session-without-syn	Enable/disable allowing TCP session without SYN flags.	option	-	disable
	<b>Option</b> <b>Description</b>			
	<i>enable</i>			Allow TCP session without SYN flags.
	<i>disable</i>			Do not allow TCP session without SYN flags.
trap-local-session *	Enable/disable local-in traffic session traps.	option	-	disable
	<b>Option</b> <b>Description</b>			
	<i>disable</i>			Disable local-in traffic session traps.
	<i>enable</i>			Enable local-in traffic session traps.
trap-session-flag *	Trap session operation flags.	option	-	tcpudp-both
	<b>Option</b> <b>Description</b>			
	<i>udp-both</i>			Trap UDP both directions.
	<i>udp-reply</i>			Trap UDP reply direction only.
	<i>tcpudp-both</i>			Trap TCP/UDP both directions.
	<i>tcpudp-reply</i>			Trap TCP/UDP reply direction only.
	<i>trap-none</i>			Do not trap anything.
utf8-spam-tagging	Enable/disable converting antispam tags to UTF-8 for better non-ASCII character support.	option	-	enable
	<b>Option</b> <b>Description</b>			
	<i>enable</i>			Convert antispam tags to UTF-8.
	<i>disable</i>			Do not convert antispam tags.
v4-ecmp-mode	IPv4 Equal-cost multi-path (ECMP) routing and load balancing mode.	option	-	source-ip-based
	<b>Option</b> <b>Description</b>			
	<i>source-ip-based</i>			Select next hop based on source IP.

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>weight-based</i>	Select next hop based on weight.		
	<i>usage-based</i>	Select next hop based on usage.		
	<i>source-dest-ip-based</i>	Select next hop based on both source and destination IPs.		
vpn-stats-log	Enable/disable periodic VPN log statistics for one or more types of VPN. Separate names with a space.	option	-	ipsec pptp l2tp ssl
	<b>Option</b>	<b>Description</b>		
	<i>ipsec</i>	IPsec.		
	<i>pptp</i>	PPTP.		
	<i>l2tp</i>	L2TP.		
	<i>ssl</i>	SSL.		
vpn-stats-period	Period to send VPN log statistics.	integer	Minimum value: 0 Maximum value: 4294967295	600
wccp-cache-engine	Enable/disable WCCP cache engine.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable WCCP cache engine.		
	<i>disable</i>	Disable WCCP cache engine.		

\* This parameter may not exist in some models.

\*\* Values may differ between models.

## config system sflow

Configure sFlow.

```
config system sflow
  Description: Configure sFlow.
  set collector-ip {ipv4-address}
  set collector-port {integer}
  set interface {string}
  set interface-select-method [auto|sdwan|...]
```

```

    set source-ip {ipv4-address}
end

```

## config system sflow

Parameter	Description	Type	Size	Default
collector-ip	IP address of the sFlow collector that sFlow agents added to interfaces in this VDOM send sFlow datagrams to.	ipv4-address	Not Specified	0.0.0.0
collector-port	UDP port number used for sending sFlow datagrams.	integer	Minimum value: 0 Maximum value: 65535	6343
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto
	Option	Description		
	auto	Set outgoing interface automatically.		
	sdwan	Set outgoing interface by SD-WAN or policy routing rules.		
	specify	Set outgoing interface manually.		
source-ip	Source IP address for sFlow agent.	ipv4-address	Not Specified	0.0.0.0

## config system sit-tunnel

Configure IPv6 tunnel over IPv4.

```

config system sit-tunnel
    Description: Configure IPv6 tunnel over IPv4.
    edit <name>
        set auto-asic-offload [enable|disable]
        set destination {ipv4-address}
        set interface {string}
        set ip6 {ipv6-prefix}
        set source {ipv4-address}
        set use-sdwan [disable|enable]
    next
end

```

## config system sit-tunnel

Parameter	Description	Type	Size	Default
auto-asic-offload *	Enable/disable tunnel ASIC offloading.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable auto ASIC offloading.		
	<i>disable</i>	Disable ASIC offloading.		
destination	Destination IP address of the tunnel.	ipv4-address	Not Specified	0.0.0.0
interface	Interface name.	string	Maximum length: 15	
ip6	IPv6 address of the tunnel.	ipv6-prefix	Not Specified	::/0
name	Tunnel name.	string	Maximum length: 15	
source	Source IP address of the tunnel.	ipv4-address	Not Specified	0.0.0.0
use-sdwan	Enable/disable use of SD-WAN to reach remote gateway.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable use of SD-WAN to reach remote gateway.		
	<i>enable</i>	Enable use of SD-WAN to reach remote gateway.		

\* This parameter may not exist in some models.

## config system smc-ntp



This command is available for model(s): FortiGate 1100E, FortiGate 1101E, FortiGate 1800F, FortiGate 1801F, FortiGate 2600F, FortiGate 2601F, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F.

It is not available for: FortiGate 1000D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1200D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 3000D, FortiGate 3100D, FortiGate 3200D, FortiGate 3700D, FortiGate 3800D, FortiGate 3960E, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 5001E1, FortiGate 5001E, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

Configure SMC NTP information.

```
config system smc-ntp
  Description: Configure SMC NTP information.
  set channel {integer}
  config ntpserver
    Description: Configure the FortiGate SMC to connect to an NTP server.
    edit <id>
      set server {ipv4-address}
    next
  end
  set ntpsync [enable|disable]
  set syncinterval {integer}
end
```

## config system smc-ntp

Parameter	Description	Type	Size	Default
channel	SMC NTP client will send NTP packets through this channel.	integer	Minimum value: 1 Maximum value: 65535	5



Parameter	Description	Type	Size	Default						
ntpsync	Enable/disable setting the FortiGate SMC system time by synchronizing with an NTP server.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable synchronization with NTP server in SMC.</td></tr><tr><td><i>disable</i></td><td>Disable synchronization with NTP server in SMC.</td></tr></table>				Option	Description	<i>enable</i>	Enable synchronization with NTP server in SMC.	<i>disable</i>	Disable synchronization with NTP server in SMC.
	Option	Description								
	<i>enable</i>	Enable synchronization with NTP server in SMC.								
<i>disable</i>	Disable synchronization with NTP server in SMC.									
syncinterval	SMC NTP synchronization interval.	integer	Minimum value: 1 Maximum value: 65535	60						

### config ntpserver

Parameter	Description	Type	Size	Default
id	NTP server ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
server	IP address of the NTP server.	ipv4-address	Not Specified	0.0.0.0

### config system sms-server

Configure SMS server for sending SMS messages to support user authentication.

```
config system sms-server
    Description: Configure SMS server for sending SMS messages to support user authentication.
    edit <name>
        set mail-server {string}
    next
end
```

### config system sms-server

Parameter	Description	Type	Size	Default
mail-server	Email-to-SMS server domain name.	string	Maximum length: 63	
name	Name of SMS server.	string	Maximum length: 35	

---

## config system snmp community

SNMP community configuration.

```
config system snmp community
    Description: SNMP community configuration.
    edit <id>
        set events {option1}, {option2}, ...
        config hosts
            Description: Configure IPv4 SNMP managers (hosts).
            edit <id>
                set source-ip {ipv4-address}
                set ip {user}
                set ha-direct [enable|disable]
                set host-type [any|query|...]
            next
        end
    config hosts6
        Description: Configure IPv6 SNMP managers.
        edit <id>
            set source-ipv6 {ipv6-address}
            set ipv6 {ipv6-prefix}
            set ha-direct [enable|disable]
            set host-type [any|query|...]
        next
    end
    set name {string}
    set query-v1-port {integer}
    set query-v1-status [enable|disable]
    set query-v2c-port {integer}
    set query-v2c-status [enable|disable]
    set status [enable|disable]
    set trap-v1-lport {integer}
    set trap-v1-rport {integer}
    set trap-v1-status [enable|disable]
    set trap-v2c-lport {integer}
    set trap-v2c-rport {integer}
    set trap-v2c-status [enable|disable]
next
end
```

---

**config system snmp community**

Parameter	Description	Type	Size	Default
events	SNMP trap events.	option	-	cpu-high mem- low log-full intf- ip vpn-tun-up vpn-tun-down ha-switch ha- hb-failure ips- signature ips- anomaly av- virus av- oversize av- pattern av- fragmented fm- if-change bgp- established bgp-backward- transition ha- member-up ha- member-down ent-conf- change av- conserve av- bypass av- oversize- passed av- oversize- blocked ips- pkg-update ips- fail-open temperature- high voltage- alert power- supply-failure faz-disconnect fan-failure wc- ap-up wc-ap- down fswctl- session-up fswctl-session- down load- balance-real- server-down per-cpu-high dhcp pool- usage ospf- nbr-state- change ospf- virtnbr-state- change **

Parameter	Description	Type	Size	Default
-----------	-------------	------	------	---------

Option	Description
<i>cpu-high</i>	Send a trap when CPU usage is high.
<i>mem-low</i>	Send a trap when available memory is low.
<i>log-full</i>	Send a trap when log disk space becomes low.
<i>intf-ip</i>	Send a trap when an interface IP address is changed.
<i>vpn-tun-up</i>	Send a trap when a VPN tunnel comes up.
<i>vpn-tun-down</i>	Send a trap when a VPN tunnel goes down.
<i>ha-switch</i>	Send a trap after an HA failover when the backup unit has taken over.
<i>ha-hb-failure</i>	Send a trap when HA heartbeats are not received.
<i>ips-signature</i>	Send a trap when IPS detects an attack.
<i>ips-anomaly</i>	Send a trap when IPS finds an anomaly.
<i>av-virus</i>	Send a trap when AntiVirus finds a virus.
<i>av-oversize</i>	Send a trap when AntiVirus finds an oversized file.
<i>av-pattern</i>	Send a trap when AntiVirus finds file matching pattern.
<i>av-fragmented</i>	Send a trap when AntiVirus finds a fragmented file.
<i>fm-if-change</i>	Send a trap when FortiManager interface changes. Send a FortiManager trap.
<i>fm-conf-change</i>	Send a trap when a configuration change is made by a FortiGate administrator and the FortiGate is managed by FortiManager.
<i>bgp-established</i>	Send a trap when a BGP FSM transitions to the established state.
<i>bgp-backward-transition</i>	Send a trap when a BGP FSM goes from a high numbered state to a lower numbered state.
<i>ha-member-up</i>	Send a trap when an HA cluster member goes up.
<i>ha-member-down</i>	Send a trap when an HA cluster member goes down.
<i>ent-conf-change</i>	Send a trap when an entity MIB change occurs (RFC4133).
<i>av-conserve</i>	Send a trap when the FortiGate enters conserve mode.
<i>av-bypass</i>	Send a trap when the FortiGate enters bypass mode.
<i>av-oversize-passed</i>	Send a trap when AntiVirus passes an oversized file.
<i>av-oversize-blocked</i>	Send a trap when AntiVirus blocks an oversized file.

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>ips-pkg-update</i>	Send a trap when the IPS signature database or engine is updated.		
	<i>ips-fail-open</i>	Send a trap when the IPS network buffer is full.		
	<i>temperature-high</i>	Send a trap when a temperature sensor registers a temperature that is too high.		
	<i>voltage-alert</i>	Send a trap when a voltage sensor registers a voltage that is outside of the normal range.		
	<i>power-supply-failure</i>	Send a trap when a power supply fails.		
	<i>faz-disconnect</i>	Send a trap when a FortiAnalyzer disconnects from the FortiGate.		
	<i>fan-failure</i>	Send a trap when a fan fails.		
	<i>wc-ap-up</i>	Send a trap when a managed FortiAP comes up.		
	<i>wc-ap-down</i>	Send a trap when a managed FortiAP goes down.		
	<i>fswctl-session-up</i>	Send a trap when a FortiSwitch controller session comes up.		
	<i>fswctl-session-down</i>	Send a trap when a FortiSwitch controller session goes down.		
	<i>load-balance-real-server-down</i>	Send a trap when a server load balance real server goes down.		
	<i>device-new</i>	Send a trap when a new device is found.		
	<i>per-cpu-high</i>	Send a trap when per-CPU usage is high.		
	<i>dhcp</i>	Send a trap when the DHCP server exhausts the IP pool, an IP address already is in use, or a DHCP client interface received a DHCP-NAK.		
<i>pool-usage</i>	Send a trap about ippool usage.			
<i>ospf-nbr-state-change</i>	Send a trap when there has been a change in the state of a non-virtual OSPF neighbor.			
<i>ospf-virtnbr-state-change</i>	Send a trap when there has been a change in the state of an OSPF virtual neighbor.			
id	Community ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
name	Community name.	string	Maximum length: 35	

Parameter	Description	Type	Size	Default						
query-v1-port	SNMP v1 query port.	integer	Minimum value: 1 Maximum value: 65535	161						
query-v1-status	Enable/disable SNMP v1 queries.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
query-v2c-port	SNMP v2c query port.	integer	Minimum value: 0 Maximum value: 65535	161						
query-v2c-status	Enable/disable SNMP v2c queries.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
status	Enable/disable this SNMP community.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
trap-v1-lport	SNMP v1 trap local port.	integer	Minimum value: 1 Maximum value: 65535	162						
trap-v1-rport	SNMP v1 trap remote port.	integer	Minimum value: 1 Maximum value: 65535	162						
trap-v1-status	Enable/disable SNMP v1 traps.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									

Parameter	Description	Type	Size	Default						
trap-v2c-lport	SNMP v2c trap local port.	integer	Minimum value: 1 Maximum value: 65535	162						
trap-v2c-rport	SNMP v2c trap remote port.	integer	Minimum value: 1 Maximum value: 65535	162						
trap-v2c-status	Enable/disable SNMP v2c traps.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>				Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									

\*\* Values may differ between models.

## config hosts

Parameter	Description	Type	Size	Default						
id	Host entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0						
source-ip	Source IPv4 address for SNMP traps.	ipv4-address	Not Specified	0.0.0.0						
ip	IPv4 address of the SNMP manager (host).	user	Not Specified							
ha-direct	Enable/disable direct management of HA cluster members.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>				Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
host-type	Control whether the SNMP manager sends SNMP queries, receives SNMP traps, or both. No traps will be sent when IP type is subnet.	option	-	any						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>any</i></td><td>Accept queries from and send traps to this SNMP manager.</td></tr></table>				Option	Description	<i>any</i>	Accept queries from and send traps to this SNMP manager.		
Option	Description									
<i>any</i>	Accept queries from and send traps to this SNMP manager.									



Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>query</i>	Accept queries from this SNMP manager but do not send traps.		
	<i>trap</i>	Send traps to this SNMP manager but do not accept SNMP queries from this SNMP manager.		

## config hosts6

Parameter	Description	Type	Size	Default
id	Host6 entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
source-ipv6	Source IPv6 address for SNMP traps.	ipv6-address	Not Specified	::
ipv6	SNMP manager IPv6 address prefix.	ipv6-prefix	Not Specified	::/0
ha-direct	Enable/disable direct management of HA cluster members.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
host-type	Control whether the SNMP manager sends SNMP queries, receives SNMP traps, or both.	option	-	any
	<b>Option</b>	<b>Description</b>		
	<i>any</i>	Accept queries from and send traps to this SNMP manager.		
	<i>query</i>	Accept queries from this SNMP manager but do not send traps.		
	<i>trap</i>	Send traps to this SNMP manager but do not accept SNMP queries from this SNMP manager.		

## config system snmp sysinfo

SNMP system info configuration.

```
config system snmp sysinfo
    Description: SNMP system info configuration.
    set contact-info {var-string}
    set description {var-string}
```

```

set engine-id {string}
set engine-id-type [text|hex|...]
set location {var-string}
set status [enable|disable]
set trap-high-cpu-threshold {integer}
set trap-log-full-threshold {integer}
set trap-low-memory-threshold {integer}
end

```

## config system snmp sysinfo

Parameter	Description	Type	Size	Default								
contact-info	Contact information.	var-string	Maximum length: 255									
description	System description.	var-string	Maximum length: 255									
engine-id	Local SNMP engineID string (maximum 27 characters).	string	Maximum length: 54									
engine-id-type	Local SNMP engineID type (text/hex/mac).	option	-	text								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>text</i></td><td>Text format.</td></tr><tr><td><i>hex</i></td><td>Octets format.</td></tr><tr><td><i>mac</i></td><td>MAC address format.</td></tr></table>	Option	Description	<i>text</i>	Text format.	<i>hex</i>	Octets format.	<i>mac</i>	MAC address format.			
Option	Description											
<i>text</i>	Text format.											
<i>hex</i>	Octets format.											
<i>mac</i>	MAC address format.											
location	System location.	var-string	Maximum length: 255									
status	Enable/disable SNMP.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
trap-high-cpu-threshold	CPU usage when trap is sent.	integer	Minimum value: 1 Maximum value: 100	80								
trap-log-full-threshold	Log disk usage when trap is sent.	integer	Minimum value: 1 Maximum value: 100	90								

Parameter	Description	Type	Size	Default
trap-low-memory-threshold	Memory usage when trap is sent.	integer	Minimum value: 1 Maximum value: 100	80

## config system snmp user

SNMP user configuration.

```

config system snmp user
    Description: SNMP user configuration.
    edit <name>
        set auth-proto [md5|sha|...]
        set auth-pwd {password}
        set events {option1}, {option2}, ...
        set ha-direct [enable|disable]
        set notify-hosts {ipv4-address}
        set notify-hosts6 {ipv6-address}
        set priv-proto [aes|des|...]
        set priv-pwd {password}
        set queries [enable|disable]
        set query-port {integer}
        set security-level [no-auth-no-priv|auth-no-priv|...]
        set source-ip {ipv4-address}
        set source-ipv6 {ipv6-address}
        set status [enable|disable]
        set trap-lport {integer}
        set trap-rport {integer}
        set trap-status [enable|disable]
    next
end

```

## config system snmp user

Parameter	Description	Type	Size	Default														
auth-proto	Authentication protocol.	option	-	sha														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>md5</i></td><td>HMAC-MD5-96 authentication protocol.</td></tr><tr><td><i>sha</i></td><td>HMAC-SHA-96 authentication protocol.</td></tr><tr><td><i>sha224</i></td><td>HMAC-SHA224 authentication protocol.</td></tr><tr><td><i>sha256</i></td><td>HMAC-SHA256 authentication protocol.</td></tr><tr><td><i>sha384</i></td><td>HMAC-SHA384 authentication protocol.</td></tr><tr><td><i>sha512</i></td><td>HMAC-SHA512 authentication protocol.</td></tr></table>				Option	Description	<i>md5</i>	HMAC-MD5-96 authentication protocol.	<i>sha</i>	HMAC-SHA-96 authentication protocol.	<i>sha224</i>	HMAC-SHA224 authentication protocol.	<i>sha256</i>	HMAC-SHA256 authentication protocol.	<i>sha384</i>	HMAC-SHA384 authentication protocol.	<i>sha512</i>	HMAC-SHA512 authentication protocol.
Option	Description																	
<i>md5</i>	HMAC-MD5-96 authentication protocol.																	
<i>sha</i>	HMAC-SHA-96 authentication protocol.																	
<i>sha224</i>	HMAC-SHA224 authentication protocol.																	
<i>sha256</i>	HMAC-SHA256 authentication protocol.																	
<i>sha384</i>	HMAC-SHA384 authentication protocol.																	
<i>sha512</i>	HMAC-SHA512 authentication protocol.																	

---

Parameter	Description	Type	Size	Default
auth-pwd	Password for authentication protocol.	password	Not Specified	

Parameter	Description	Type	Size	Default
events	SNMP notifications (traps) to send.	option	-	cpu-high mem- low log-full intf- ip vpn-tun-up vpn-tun-down ha-switch ha- hb-failure ips- signature ips- anomaly av- virus av- oversize av- pattern av- fragmented fm- if-change bgp- established bgp-backward- transition ha- member-up ha- member-down ent-conf- change av- conserve av- bypass av- oversize- passed av- oversize- blocked ips- pkg-update ips- fail-open temperature- high voltage- alert power- supply-failure faz-disconnect fan-failure wc- ap-up wc-ap- down fswctl- session-up fswctl-session- down load- balance-real- server-down per-cpu-high dhcp pool- usage ospf- nbr-state- change ospf- virtnbr-state- change **

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>cpu-high</i>	Send a trap when CPU usage is high.		
	<i>mem-low</i>	Send a trap when available memory is low.		
	<i>log-full</i>	Send a trap when log disk space becomes low.		
	<i>intf-ip</i>	Send a trap when an interface IP address is changed.		
	<i>vpn-tun-up</i>	Send a trap when a VPN tunnel comes up.		
	<i>vpn-tun-down</i>	Send a trap when a VPN tunnel goes down.		
	<i>ha-switch</i>	Send a trap after an HA failover when the backup unit has taken over.		
	<i>ha-hb-failure</i>	Send a trap when HA heartbeats are not received.		
	<i>ips-signature</i>	Send a trap when IPS detects an attack.		
	<i>ips-anomaly</i>	Send a trap when IPS finds an anomaly.		
	<i>av-virus</i>	Send a trap when AntiVirus finds a virus.		
	<i>av-oversize</i>	Send a trap when AntiVirus finds an oversized file.		
	<i>av-pattern</i>	Send a trap when AntiVirus finds file matching pattern.		
	<i>av-fragmented</i>	Send a trap when AntiVirus finds a fragmented file.		
	<i>fm-if-change</i>	Send a trap when FortiManager interface changes. Send a FortiManager trap.		
	<i>fm-conf-change</i>	Send a trap when a configuration change is made by a FortiGate administrator and the FortiGate is managed by FortiManager.		
	<i>bgp-established</i>	Send a trap when a BGP FSM transitions to the established state.		
	<i>bgp-backward-transition</i>	Send a trap when a BGP FSM goes from a high numbered state to a lower numbered state.		
	<i>ha-member-up</i>	Send a trap when an HA cluster member goes up.		
	<i>ha-member-down</i>	Send a trap when an HA cluster member goes down.		
	<i>ent-conf-change</i>	Send a trap when an entity MIB change occurs (RFC4133).		
	<i>av-conserve</i>	Send a trap when the FortiGate enters conserve mode.		
	<i>av-bypass</i>	Send a trap when the FortiGate enters bypass mode.		
	<i>av-oversize-passed</i>	Send a trap when AntiVirus passes an oversized file.		
	<i>av-oversize-blocked</i>	Send a trap when AntiVirus blocks an oversized file.		

Parameter	Description	Type	Size	Default																																							
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ips-pkg-update</i></td><td>Send a trap when the IPS signature database or engine is updated.</td></tr><tr><td><i>ips-fail-open</i></td><td>Send a trap when the IPS network buffer is full.</td></tr><tr><td><i>temperature-high</i></td><td>Send a trap when a temperature sensor registers a temperature that is too high.</td></tr><tr><td><i>voltage-alert</i></td><td>Send a trap when a voltage sensor registers a voltage that is outside of the normal range.</td></tr><tr><td><i>power-supply-failure</i></td><td>Send a trap when a power supply fails.</td></tr><tr><td><i>faz-disconnect</i></td><td>Send a trap when a FortiAnalyzer disconnects from the FortiGate.</td></tr><tr><td><i>fan-failure</i></td><td>Send a trap when a fan fails.</td></tr><tr><td><i>wc-ap-up</i></td><td>Send a trap when a managed FortiAP comes up.</td></tr><tr><td><i>wc-ap-down</i></td><td>Send a trap when a managed FortiAP goes down.</td></tr><tr><td><i>fswctl-session-up</i></td><td>Send a trap when a FortiSwitch controller session comes up.</td></tr><tr><td><i>fswctl-session-down</i></td><td>Send a trap when a FortiSwitch controller session goes down.</td></tr><tr><td><i>load-balance-real-server-down</i></td><td>Send a trap when a server load balance real server goes down.</td></tr><tr><td><i>device-new</i></td><td>Send a trap when a new device is found.</td></tr><tr><td><i>per-cpu-high</i></td><td>Send a trap when per-CPU usage is high.</td></tr><tr><td><i>dhcp</i></td><td>Send a trap when the DHCP server exhausts the IP pool, an IP address already is in use, or a DHCP client interface received a DHCP-NAK.</td></tr><tr><td><i>pool-usage</i></td><td>Send a trap about ippool usage.</td></tr><tr><td><i>ospf-nbr-state-change</i></td><td>Send a trap when there has been a change in the state of a non-virtual OSPF neighbor.</td></tr><tr><td><i>ospf-virtnbr-state-change</i></td><td>Send a trap when there has been a change in the state of an OSPF virtual neighbor.</td></tr></table>	Option	Description	<i>ips-pkg-update</i>	Send a trap when the IPS signature database or engine is updated.	<i>ips-fail-open</i>	Send a trap when the IPS network buffer is full.	<i>temperature-high</i>	Send a trap when a temperature sensor registers a temperature that is too high.	<i>voltage-alert</i>	Send a trap when a voltage sensor registers a voltage that is outside of the normal range.	<i>power-supply-failure</i>	Send a trap when a power supply fails.	<i>faz-disconnect</i>	Send a trap when a FortiAnalyzer disconnects from the FortiGate.	<i>fan-failure</i>	Send a trap when a fan fails.	<i>wc-ap-up</i>	Send a trap when a managed FortiAP comes up.	<i>wc-ap-down</i>	Send a trap when a managed FortiAP goes down.	<i>fswctl-session-up</i>	Send a trap when a FortiSwitch controller session comes up.	<i>fswctl-session-down</i>	Send a trap when a FortiSwitch controller session goes down.	<i>load-balance-real-server-down</i>	Send a trap when a server load balance real server goes down.	<i>device-new</i>	Send a trap when a new device is found.	<i>per-cpu-high</i>	Send a trap when per-CPU usage is high.	<i>dhcp</i>	Send a trap when the DHCP server exhausts the IP pool, an IP address already is in use, or a DHCP client interface received a DHCP-NAK.	<i>pool-usage</i>	Send a trap about ippool usage.	<i>ospf-nbr-state-change</i>	Send a trap when there has been a change in the state of a non-virtual OSPF neighbor.	<i>ospf-virtnbr-state-change</i>	Send a trap when there has been a change in the state of an OSPF virtual neighbor.				
	Option	Description																																									
	<i>ips-pkg-update</i>	Send a trap when the IPS signature database or engine is updated.																																									
	<i>ips-fail-open</i>	Send a trap when the IPS network buffer is full.																																									
	<i>temperature-high</i>	Send a trap when a temperature sensor registers a temperature that is too high.																																									
	<i>voltage-alert</i>	Send a trap when a voltage sensor registers a voltage that is outside of the normal range.																																									
	<i>power-supply-failure</i>	Send a trap when a power supply fails.																																									
	<i>faz-disconnect</i>	Send a trap when a FortiAnalyzer disconnects from the FortiGate.																																									
	<i>fan-failure</i>	Send a trap when a fan fails.																																									
	<i>wc-ap-up</i>	Send a trap when a managed FortiAP comes up.																																									
	<i>wc-ap-down</i>	Send a trap when a managed FortiAP goes down.																																									
	<i>fswctl-session-up</i>	Send a trap when a FortiSwitch controller session comes up.																																									
	<i>fswctl-session-down</i>	Send a trap when a FortiSwitch controller session goes down.																																									
	<i>load-balance-real-server-down</i>	Send a trap when a server load balance real server goes down.																																									
	<i>device-new</i>	Send a trap when a new device is found.																																									
	<i>per-cpu-high</i>	Send a trap when per-CPU usage is high.																																									
	<i>dhcp</i>	Send a trap when the DHCP server exhausts the IP pool, an IP address already is in use, or a DHCP client interface received a DHCP-NAK.																																									
<i>pool-usage</i>	Send a trap about ippool usage.																																										
<i>ospf-nbr-state-change</i>	Send a trap when there has been a change in the state of a non-virtual OSPF neighbor.																																										
<i>ospf-virtnbr-state-change</i>	Send a trap when there has been a change in the state of an OSPF virtual neighbor.																																										
ha-direct	Enable/disable direct management of HA cluster members.	option	-	disable																																							
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.																																				
	Option	Description																																									
	<i>enable</i>	Enable setting.																																									
<i>disable</i>	Disable setting.																																										

Parameter	Description	Type	Size	Default										
name	SNMP user name.	string	Maximum length: 32											
notify-hosts	SNMP managers to send notifications (traps) to.	ipv4-address	Not Specified											
notify-hosts6	IPv6 SNMP managers to send notifications (traps) to.	ipv6-address	Not Specified											
priv-proto	Privacy (encryption) protocol.	option	-	aes										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>aes</td><td>CFB128-AES-128 symmetric encryption protocol.</td></tr><tr><td>des</td><td>CBC-DES symmetric encryption protocol.</td></tr><tr><td>aes256</td><td>CFB128-AES-256 symmetric encryption protocol.</td></tr><tr><td>aes256cisco</td><td>CFB128-AES-256 symmetric encryption protocol compatible with CISCO.</td></tr></table>	Option	Description	aes	CFB128-AES-128 symmetric encryption protocol.	des	CBC-DES symmetric encryption protocol.	aes256	CFB128-AES-256 symmetric encryption protocol.	aes256cisco	CFB128-AES-256 symmetric encryption protocol compatible with CISCO.			
Option	Description													
aes	CFB128-AES-128 symmetric encryption protocol.													
des	CBC-DES symmetric encryption protocol.													
aes256	CFB128-AES-256 symmetric encryption protocol.													
aes256cisco	CFB128-AES-256 symmetric encryption protocol compatible with CISCO.													
priv-pwd	Password for privacy (encryption) protocol.	password	Not Specified											
queries	Enable/disable SNMP queries for this user.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>	Option	Description	enable	Enable setting.	disable	Disable setting.							
Option	Description													
enable	Enable setting.													
disable	Disable setting.													
query-port	SNMPv3 query port.	integer	Minimum value: 0 Maximum value: 65535	161										
security-level	Security level for message authentication and encryption.	option	-	no-auth-no-priv										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>no-auth-no-priv</td><td>Message with no authentication and no privacy (encryption).</td></tr><tr><td>auth-no-priv</td><td>Message with authentication but no privacy (encryption).</td></tr><tr><td>auth-priv</td><td>Message with authentication and privacy (encryption).</td></tr></table>	Option	Description	no-auth-no-priv	Message with no authentication and no privacy (encryption).	auth-no-priv	Message with authentication but no privacy (encryption).	auth-priv	Message with authentication and privacy (encryption).					
Option	Description													
no-auth-no-priv	Message with no authentication and no privacy (encryption).													
auth-no-priv	Message with authentication but no privacy (encryption).													
auth-priv	Message with authentication and privacy (encryption).													
source-ip	Source IP for SNMP trap.	ipv4-address	Not Specified	0.0.0.0										
source-ipv6	Source IPv6 for SNMP trap.	ipv6-address	Not Specified	::										



Parameter	Description	Type	Size	Default						
status	Enable/disable this SNMP user.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>				Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.
	Option	Description								
	<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.									
trap-lport	SNMPv3 local trap port.	integer	Minimum value: 0 Maximum value: 65535	162						
trap-rport	SNMPv3 trap remote port.	integer	Minimum value: 0 Maximum value: 65535	162						
trap-status	Enable/disable traps for this SNMP user.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>				Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.
	Option	Description								
	<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.									

\*\* Values may differ between models.

## config system speed-test-schedule

Speed test schedule for each interface.

```

config system speed-test-schedule
    Description: Speed test schedule for each interface.
    edit <interface>
        set diffserv {user}
        set dynamic-server [disable|enable]
        set schedules <name1>, <name2>, ...
        set server-name {string}
        set status [disable|enable]
        set update-inbandwidth [disable|enable]
        set update-inbandwidth-maximum {integer}
        set update-inbandwidth-minimum {integer}
        set update-outbandwidth [disable|enable]
        set update-outbandwidth-maximum {integer}
        set update-outbandwidth-minimum {integer}
    next
end

```

## config system speed-test-schedule

Parameter	Description	Type	Size	Default
diffserv	DSCP used for speed test.	user	Not Specified	
dynamic-server	Enable/disable dynamic server option.	option	-	disable
	Option	Description		
	disable	Disable dynamic server.		
	enable	Enable dynamic server.The speed test server will be found automatically.		
interface	Interface name.	string	Maximum length: 35	
schedules <name>	Schedules for the interface. Name of a firewall recurring schedule.	string	Maximum length: 31	
server-name	Speed test server name.	string	Maximum length: 35	
status	Enable/disable scheduled speed test.	option	-	enable
	Option	Description		
	disable	Disable scheduled speed test.		
	enable	Enable scheduled speed test.		
update-inbandwidth	Enable/disable bypassing interface's inbound bandwidth setting.	option	-	disable
	Option	Description		
	disable	Honor interface's inbandwidth shaping.		
	enable	Ignore interface's inbandwidth shaping.		
update-inbandwidth-maximum	Maximum downloading bandwidth (kbps) to be used in a speed test.	integer	Minimum value: 0 Maximum value: 16776000	0
update-inbandwidth-minimum	Minimum downloading bandwidth (kbps) to be considered effective.	integer	Minimum value: 0 Maximum value: 16776000	0
update-outbandwidth	Enable/disable bypassing interface's outbound bandwidth setting.	option	-	disable

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Honor interface's outbandwidth shaping.		
	<i>enable</i>	Ignore updating interface's outbandwidth shaping.		
update-outbandwidth-maximum	Maximum uploading bandwidth (kbps) to be used in a speed test.	integer	Minimum value: 0 Maximum value: 16776000	0
update-outbandwidth-minimum	Minimum uploading bandwidth (kbps) to be considered effective.	integer	Minimum value: 0 Maximum value: 16776000	0

## config system speed-test-server



The `config system speed-test-server` command is read-only. Administrators cannot configure custom servers.

Configure speed test server list.

```

config system speed-test-server
  Description: Configure speed test server list.
  edit <name>
    config host
      Description: Hosts of the server.
      edit <id>
        set ip {ipv4-address}
        set port {integer}
        set user {string}
        set password {password}
        set longitude {string}
        set latitude {string}
        set distance {integer}
      next
    end
    set timestamp {integer}
  next
end

```

## config system speed-test-server

Parameter	Description	Type	Size	Default
name	Speed test server name.	string	Maximum length: 35	
timestamp	Speed test server timestamp.	integer	Minimum value: 0 Maximum value: 4294967295	0

## config host

Parameter	Description	Type	Size	Default
id	Server host ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
ip	Server host IPv4 address.	ipv4-address	Not Specified	0.0.0.0
port	Server host port number to communicate with client.	integer	Minimum value: 1 Maximum value: 65535	5204
user	Speed test host user name.	string	Maximum length: 64	
password	Speed test host password.	password	Not Specified	
longitude	Speed test host longitude.	string	Maximum length: 7	
latitude	Speed test host latitude.	string	Maximum length: 7	
distance	Speed test host distance.	integer	Minimum value: 0 Maximum value: 4294967295	0

## config system sso-admin

Configure SSO admin users.

```

config system sso-admin
    Description: Configure SSO admin users.
    edit <name>
        set accprofile {string}
        set vdom <name1>, <name2>, ...
    next
end

```

## config system sso-admin

Parameter	Description	Type	Size	Default
accprofile	SSO admin user access profile.	string	Maximum length: 35	
name	SSO admin name.	string	Maximum length: 64	
vdom <name>	Virtual domain(s) that the administrator can access. Virtual domain name.	string	Maximum length: 79	

## config system sso-forticloud-admin

Configure FortiCloud SSO admin users.

```

config system sso-forticloud-admin
    Description: Configure FortiCloud SSO admin users.
    edit <name>
        set vdom <name1>, <name2>, ...
    next
end

```

## config system sso-forticloud-admin

Parameter	Description	Type	Size	Default
name	FortiCloud SSO admin name.	string	Maximum length: 64	
vdom <name>	Virtual domain(s) that the administrator can access. Virtual domain name.	string	Maximum length: 79	

## config system standalone-cluster

Configure FortiGate Session Life Support Protocol (FGSP) cluster attributes.

```

config system standalone-cluster
    Description: Configure FortiGate Session Life Support Protocol (FGSP) cluster attributes.
    set encryption [enable|disable]

```

```

set group-member-id {integer}
set layer2-connection [available|unavailable]
set psksecret {password-3}
set session-sync-dev {user}
set standalone-group-id {integer}
end

```

## config system standalone-cluster

Parameter	Description	Type	Size	Default						
encryption	Enable/disable encryption when synchronizing sessions.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable encryption when synchronizing sessions.</td></tr><tr><td><i>disable</i></td><td>Disable encryption when synchronizing sessions.</td></tr></table>	Option	Description	<i>enable</i>	Enable encryption when synchronizing sessions.	<i>disable</i>	Disable encryption when synchronizing sessions.			
Option	Description									
<i>enable</i>	Enable encryption when synchronizing sessions.									
<i>disable</i>	Disable encryption when synchronizing sessions.									
group-member-id	Cluster member ID.	integer	Minimum value: 0 Maximum value: 15	0						
layer2-connection	Indicate whether layer 2 connections are present among FGSP members.	option	-	unavailable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>available</i></td><td>There exist layer 2 connections among FGSP members.</td></tr><tr><td><i>unavailable</i></td><td>There does not exist layer 2 connection among FGSP members.</td></tr></table>	Option	Description	<i>available</i>	There exist layer 2 connections among FGSP members.	<i>unavailable</i>	There does not exist layer 2 connection among FGSP members.			
Option	Description									
<i>available</i>	There exist layer 2 connections among FGSP members.									
<i>unavailable</i>	There does not exist layer 2 connection among FGSP members.									
psksecret	Pre-shared secret for session synchronization (ASCII string or hexadecimal encoded with a leading 0x).	password-3	Not Specified							
session-sync-dev	Offload session-sync process to kernel and sync sessions using connected interface(s) directly.	user	Not Specified							
standalone-group-id	Cluster group ID. Must be the same for all members.	integer	Minimum value: 0 Maximum value: 255	0						

## config system storage

Configure logical storage.

```

config system storage
    Description: Configure logical storage.
    edit <name>
        set device {string}
    end
end

```

```

    set media-status [enable|disable|...]
    set order {integer}
    set partition {string}
    set size {integer}
    set status [enable|disable]
    set usage [log|wanopt]
    set wanopt-mode [mix|wanopt|...]
next
end

```

## config system storage

Parameter	Description	Type	Size	Default
device	Partition device.	string	Maximum length: 19	?
media-status	The physical status of current media.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Storage is enabled.		
	<i>disable</i>	Storage is disabled.		
	<i>fail</i>	Storage have some fail sector.		
name	Storage name.	string	Maximum length: 35	default_n
order	Set storage order.	integer	Minimum value: 0 Maximum value: 255	0
partition	Label of underlying partition.	string	Maximum length: 16	<unknown>
size	Partition size.	integer	Minimum value: 0 Maximum value: 4294967295	0
status	Enable/disable storage.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
usage	Use hard disk for logging or WAN Optimization.	option	-	log

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>log</i>	Use hard disk for logging.		
	<i>wanopt</i>	Use hard disk for WAN Optimization.		
wanopt-mode *	WAN Optimization mode.	option	-	mix
	<b>Option</b>	<b>Description</b>		
	<i>mix</i>	Use hard disk for WAN Optimization mix mode.		
	<i>wanopt</i>	Use hard disk for WAN Optimization wanopt mode.		
	<i>webcache</i>	Use hard disk for WAN Optimization webcache mode.		

\* This parameter may not exist in some models.

## config system stp



This command is available for model(s): FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 140E-POE, FortiGate 140E, FortiGate 1800F, FortiGate 1801F, FortiGate 200F, FortiGate 201F, FortiGate 2600F, FortiGate 2601F, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3500F, FortiGate 3501F, FortiGate 3800D, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 600F, FortiGate 601F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 90E, FortiGate 91E, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 1000D, FortiGate 1200D, FortiGate 1500DT, FortiGate 1500D, FortiGate 2000E, FortiGate 200E, FortiGate 201E, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 3000D, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 601E, FortiGate 800D, FortiGate 900D, FortiGate VM64.

Configure Spanning Tree Protocol (STP).

```
config system stp
    Description: Configure Spanning Tree Protocol (STP).
    set forward-delay {integer}
```



```

set hello-time {integer}
set max-age {integer}
set max-hops {integer}
set switch-priority [0|4096|...]
end

```

## config system stp

Parameter	Description	Type	Size	Default																				
forward-delay	Forward delay.	integer	Minimum value: 4 Maximum value: 30	15																				
hello-time	Hello time.	integer	Minimum value: 1 Maximum value: 10	2																				
max-age	Maximum packet age.	integer	Minimum value: 6 Maximum value: 40	20																				
max-hops	Maximum number of hops.	integer	Minimum value: 1 Maximum value: 40	20																				
switch-priority	STP switch priority; the lower the number the higher the priority (select from 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, and 57344).	option	-	32768																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>0</td><td>0</td></tr><tr><td>4096</td><td>4096</td></tr><tr><td>8192</td><td>8192</td></tr><tr><td>12288</td><td>12288</td></tr><tr><td>16384</td><td>16384</td></tr><tr><td>20480</td><td>20480</td></tr><tr><td>24576</td><td>24576</td></tr><tr><td>28672</td><td>28672</td></tr><tr><td>32768</td><td>32768</td></tr></table>				Option	Description	0	0	4096	4096	8192	8192	12288	12288	16384	16384	20480	20480	24576	24576	28672	28672	32768	32768
Option	Description																							
0	0																							
4096	4096																							
8192	8192																							
12288	12288																							
16384	16384																							
20480	20480																							
24576	24576																							
28672	28672																							
32768	32768																							

Parameter	Description	Type	Size	Default
	Option	Description		
	36864	36864		
	40960	40960		
	45056	45056		
	49152	49152		
	53248	53248		
	57344	57344		

## config system switch-interface

Configure software switch interfaces by grouping physical and WiFi interfaces.

```
config system switch-interface
    Description: Configure software switch interfaces by grouping physical and WiFi
    interfaces.
    edit <name>
        set intra-switch-policy [implicit|explicit]
        set mac-ttl {integer}
        set member <interface-name1>, <interface-name2>, ...
        set span [disable|enable]
        set span-dest-port {string}
        set span-direction [rx|tx|...]
        set span-source-port <interface-name1>, <interface-name2>, ...
        set type [switch|hub]
        set vdom {string}
    next
end
```

## config system switch-interface

Parameter	Description	Type	Size	Default
intra-switch-policy	Allow any traffic between switch interfaces or require firewall policies to allow traffic between switch interfaces.	option	-	implicit
	Option	Description		
	<i>implicit</i>	Traffic between switch members is implicitly allowed.		
	<i>explicit</i>	Traffic between switch members must match firewall policies.		

Parameter	Description	Type	Size	Default								
mac-ttl	Duration for which MAC addresses are held in the ARP table.	integer	Minimum value: 300 Maximum value: 8640000	300								
member <interface-name>	Names of the interfaces that belong to the virtual switch. Physical interface name.	string	Maximum length: 79									
name	Interface name (name cannot be in use by any other interfaces, VLANs, or inter-VDOM links).	string	Maximum length: 15									
span	Enable/disable port spanning. Port spanning echoes traffic received by the software switch to the span destination port.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable port spanning.</td></tr><tr><td><i>enable</i></td><td>Enable port spanning.</td></tr></table>				Option	Description	<i>disable</i>	Disable port spanning.	<i>enable</i>	Enable port spanning.		
Option	Description											
<i>disable</i>	Disable port spanning.											
<i>enable</i>	Enable port spanning.											
span-dest-port	SPAN destination port name. All traffic on the SPAN source ports is echoed to the SPAN destination port.	string	Maximum length: 15									
span-direction	The direction in which the SPAN port operates, either: rx, tx, or both.	option	-	both								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>rx</i></td><td>Copies only received packets from source SPAN ports to the destination SPAN port.</td></tr><tr><td><i>tx</i></td><td>Copies only transmitted packets from source SPAN ports to the destination SPAN port.</td></tr><tr><td><i>both</i></td><td>Copies both received and transmitted packets from source SPAN ports to the destination SPAN port.</td></tr></table>				Option	Description	<i>rx</i>	Copies only received packets from source SPAN ports to the destination SPAN port.	<i>tx</i>	Copies only transmitted packets from source SPAN ports to the destination SPAN port.	<i>both</i>	Copies both received and transmitted packets from source SPAN ports to the destination SPAN port.
Option	Description											
<i>rx</i>	Copies only received packets from source SPAN ports to the destination SPAN port.											
<i>tx</i>	Copies only transmitted packets from source SPAN ports to the destination SPAN port.											
<i>both</i>	Copies both received and transmitted packets from source SPAN ports to the destination SPAN port.											
span-source-port <interface-name>	Physical interface name. Port spanning echoes all traffic on the SPAN source ports to the SPAN destination port. Physical interface name.	string	Maximum length: 79									
type	Type of switch based on functionality: switch for normal functionality, or hub to duplicate packets to all port members.	option	-	switch								

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>switch</i>	Switch for normal switch functionality (available in NAT mode only).		
	<i>hub</i>	Hub to duplicate packets to all member ports.		
vdom	VDOM that the software switch belongs to.	string	Maximum length: 31	

## config system tos-based-priority

Configure Type of Service (ToS) based priority table to set network traffic priorities.

```
config system tos-based-priority
    Description: Configure Type of Service (ToS) based priority table to set network traffic
priorities.
    edit <id>
        set priority [low|medium|...]
        set tos {integer}
    next
end
```

## config system tos-based-priority

Parameter	Description	Type	Size	Default
id	Item ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
priority	ToS based priority level to low, medium or high.	option	-	high
	<b>Option</b>	<b>Description</b>		
	<i>low</i>	Low priority.		
	<i>medium</i>	Medium priority.		
	<i>high</i>	High priority.		
tos	Value of the ToS byte in the IP datagram header.	integer	Minimum value: 0 Maximum value: 15	0

## config system vdom-dns

Configure DNS servers for a non-management VDOM.

```
config system vdom-dns
    Description: Configure DNS servers for a non-management VDOM.
    set alt-primary {ipv4-address}
    set alt-secondary {ipv4-address}
    set interface {string}
    set interface-select-method [auto|sdwan|...]
    set ip6-primary {ipv6-address}
    set ip6-secondary {ipv6-address}
    set primary {ipv4-address}
    set protocol {option1}, {option2}, ...
    set secondary {ipv4-address}
    set server-hostname <hostname1>, <hostname2>, ...
    set server-select-method [least-rtt|failover]
    set source-ip {ipv4-address}
    set ssl-certificate {string}
    set vdom-dns [enable|disable]
end
```

## config system vdom-dns

Parameter	Description	Type	Size	Default								
alt-primary	Alternate primary DNS server. This is not used as a failover DNS server.	ipv4-address	Not Specified	0.0.0.0								
alt-secondary	Alternate secondary DNS server. This is not used as a failover DNS server.	ipv4-address	Not Specified	0.0.0.0								
interface	Specify outgoing interface to reach server.	string	Maximum length: 15									
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>auto</td><td>Set outgoing interface automatically.</td></tr><tr><td>sdwan</td><td>Set outgoing interface by SD-WAN or policy routing rules.</td></tr><tr><td>specify</td><td>Set outgoing interface manually.</td></tr></table>				Option	Description	auto	Set outgoing interface automatically.	sdwan	Set outgoing interface by SD-WAN or policy routing rules.	specify	Set outgoing interface manually.
	Option	Description										
	auto	Set outgoing interface automatically.										
	sdwan	Set outgoing interface by SD-WAN or policy routing rules.										
specify	Set outgoing interface manually.											
ip6-primary	Primary IPv6 DNS server IP address for the VDOM.	ipv6-address	Not Specified	::								
ip6-secondary	Secondary IPv6 DNS server IP address for the VDOM.	ipv6-address	Not Specified	::								
primary	Primary DNS server IP address for the VDOM.	ipv4-address	Not Specified	0.0.0.0								

Parameter	Description	Type	Size	Default								
protocol	DNS transport protocols.	option	-	cleartext								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>cleartext</i></td><td>DNS over UDP/53, DNS over TCP/53.</td></tr><tr><td><i>dot</i></td><td>DNS over TLS/853.</td></tr><tr><td><i>doh</i></td><td>DNS over HTTPS/443.</td></tr></table>	Option	Description	<i>cleartext</i>	DNS over UDP/53, DNS over TCP/53.	<i>dot</i>	DNS over TLS/853.	<i>doh</i>	DNS over HTTPS/443.			
	Option	Description										
	<i>cleartext</i>	DNS over UDP/53, DNS over TCP/53.										
	<i>dot</i>	DNS over TLS/853.										
<i>doh</i>	DNS over HTTPS/443.											
secondary	Secondary DNS server IP address for the VDOM.	ipv4-address	Not Specified	0.0.0.0								
server-hostname <hostname>	DNS server host name list. DNS server host name list separated by space (maximum 4 domains).	string	Maximum length: 127									
server-select-method	Specify how configured servers are prioritized.	option	-	least-rtt								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>least-rtt</i></td><td>Select servers based on least round trip time.</td></tr><tr><td><i>failover</i></td><td>Select servers based on the order they are configured.</td></tr></table>	Option	Description	<i>least-rtt</i>	Select servers based on least round trip time.	<i>failover</i>	Select servers based on the order they are configured.					
	Option	Description										
	<i>least-rtt</i>	Select servers based on least round trip time.										
<i>failover</i>	Select servers based on the order they are configured.											
source-ip	Source IP for communications with the DNS server.	ipv4-address	Not Specified	0.0.0.0								
ssl-certificate	Name of local certificate for SSL connections.	string	Maximum length: 35	Fortinet_Factory								
vdom-dns	Enable/disable configuring DNS servers for the current VDOM.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable configuring DNS servers for the current VDOM.</td></tr><tr><td><i>disable</i></td><td>Disable configuring DNS servers for the current VDOM.</td></tr></table>	Option	Description	<i>enable</i>	Enable configuring DNS servers for the current VDOM.	<i>disable</i>	Disable configuring DNS servers for the current VDOM.					
	Option	Description										
	<i>enable</i>	Enable configuring DNS servers for the current VDOM.										
<i>disable</i>	Disable configuring DNS servers for the current VDOM.											

## config system vdom-exception

Global configuration objects that can be configured independently across different ha peers for all VDOMs or for the defined VDOM scope.

```
config system vdom-exception
```

Description: Global configuration objects that can be configured independently across different ha peers for all VDOMs or for the defined VDOM scope.

```
edit <id>
    set object [log.fortianalyzer.setting|log.fortianalyzer.override-setting|...]
    set scope [all|inclusive|...]
    set vdom <name1>, <name2>, ...
```

next  
end

## config system vdom-exception

Parameter	Description	Type	Size	Default
id	Index.	integer	Minimum value: 1 Maximum value: 4096	0
object	Name of the configuration object that can be configured independently for all VDOMs.	option	-	

Option	Description
<i>log.fortianalyzer.setting</i>	log.fortianalyzer.setting
<i>log.fortianalyzer.override-setting</i>	log.fortianalyzer.override-setting
<i>log.fortianalyzer2.setting</i>	log.fortianalyzer2.setting
<i>log.fortianalyzer2.override-setting</i>	log.fortianalyzer2.override-setting
<i>log.fortianalyzer3.setting</i>	log.fortianalyzer3.setting
<i>log.fortianalyzer3.override-setting</i>	log.fortianalyzer3.override-setting
<i>log.fortianalyzer-cloud.setting</i>	log.fortianalyzer-cloud.setting
<i>log.fortianalyzer-cloud.override-setting</i>	log.fortianalyzer-cloud.override-setting
<i>log.syslogd.setting</i>	log.syslogd.setting
<i>log.syslogd.override-setting</i>	log.syslogd.override-setting
<i>log.syslogd2.setting</i>	log.syslogd2.setting
<i>log.syslogd2.override-setting</i>	log.syslogd2.override-setting
<i>log.syslogd3.setting</i>	log.syslogd3.setting
<i>log.syslogd3.override-setting</i>	log.syslogd3.override-setting
<i>log.syslogd4.setting</i>	log.syslogd4.setting
<i>log.syslogd4.override-setting</i>	log.syslogd4.override-setting
<i>system.gre-tunnel</i>	system.gre-tunnel
<i>system.central-management</i>	system.central-management

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>system.csf</i>	system.csf		
	<i>user.radius</i>	user.radius		
scope	Determine whether the configuration object can be configured separately for all VDOMs or if some VDOMs share the same configuration.	option	-	all
	<b>Option</b>	<b>Description</b>		
	<i>all</i>	Object configuration independent for all VDOMs.		
	<i>inclusive</i>	Object configuration independent for the listed VDOMs. Other VDOMs use the global configuration.		
	<i>exclusive</i>	Use the global object configuration for the listed VDOMs. Other VDOMs can be configured independently.		
vdom <name>	Names of the VDOMs. VDOM name.	string	Maximum length: 79	

## config system vdom-link

Configure VDOM links.

```
config system vdom-link
    Description: Configure VDOM links.
    edit <name>
        set type [ppp|ethernet|...]
        set vcluster [vcluster1|vcluster2]
    next
end
```

## config system vdom-link

Parameter	Description	Type	Size	Default				
name	VDOM link name (maximum = 11 characters).	string	Maximum length: 11					
type	VDOM link type: PPP or Ethernet.	option	-	ppp				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ppp</i></td><td>PPP VDOM link.</td></tr></table>				Option	Description	<i>ppp</i>	PPP VDOM link.
Option	Description							
<i>ppp</i>	PPP VDOM link.							



Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>ethernet</i>	Ethernet VDOM link.		
	<i>npupair</i>	NPU VDOM link.		
vcluster	Virtual cluster.	option	-	vcluster1
	<b>Option</b>	<b>Description</b>		
	<i>vcluster1</i>	Virtual cluster 1.		
	<i>vcluster2</i>	Virtual cluster 2.		

## config system vdom-netflow

Configure NetFlow per VDOM.

```
config system vdom-netflow
    Description: Configure NetFlow per VDOM.
    set collector-ip {ipv4-address}
    set collector-port {integer}
    set interface {string}
    set interface-select-method [auto|sdwan|...]
    set source-ip {ipv4-address}
    set vdom-netflow [enable|disable]
end
```

## config system vdom-netflow

Parameter	Description	Type	Size	Default
collector-ip	NetFlow collector IP address.	ipv4-address	Not Specified	0.0.0.0
collector-port	NetFlow collector port number.	integer	Minimum value: 0 Maximum value: 65535	2055
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto
	<b>Option</b>	<b>Description</b>		
	<i>auto</i>	Set outgoing interface automatically.		

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.		
	<i>specify</i>	Set outgoing interface manually.		
source-ip	Source IP address for communication with the NetFlow agent.	ipv4-address	Not Specified	0.0.0.0
vdom-netflow	Enable/disable NetFlow per VDOM.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable NetFlow per VDOM.		
	<i>disable</i>	Disable NetFlow per VDOM.		

## config system vdom-property

Configure VDOM property.

```

config system vdom-property
  Description: Configure VDOM property.
  edit <name>
    set custom-service {user}
    set description {string}
    set dialup-tunnel {user}
    set firewall-address {user}
    set firewall-addrgrp {user}
    set firewall-policy {user}
    set ipsec-phase1 {user}
    set ipsec-phase1-interface {user}
    set ipsec-phase2 {user}
    set ipsec-phase2-interface {user}
    set log-disk-quota {user}
    set onetime-schedule {user}
    set proxy {user}
    set recurring-schedule {user}
    set service-group {user}
    set session {user}
    set snmp-index {integer}
    set sslvpn {user}
    set user {user}
    set user-group {user}
  next
end

```

## config system vdom-property

Parameter	Description	Type	Size	Default
custom-service	Maximum guaranteed number of firewall custom services.	user	Not Specified	
description	Description.	string	Maximum length: 127	
dialup-tunnel	Maximum guaranteed number of dial-up tunnels.	user	Not Specified	
firewall-address	Maximum guaranteed number of firewall addresses (IPv4, IPv6, multicast).	user	Not Specified	
firewall-addrgroup	Maximum guaranteed number of firewall address groups (IPv4, IPv6).	user	Not Specified	
firewall-policy	Maximum guaranteed number of firewall policies (policy, DoS-policy4, DoS-policy6, multicast).	user	Not Specified	
ipsec-phase1	Maximum guaranteed number of VPN IPsec phase 1 tunnels.	user	Not Specified	
ipsec-phase1-interface	Maximum guaranteed number of VPN IPsec phase1 interface tunnels.	user	Not Specified	
ipsec-phase2	Maximum guaranteed number of VPN IPsec phase 2 tunnels.	user	Not Specified	
ipsec-phase2-interface	Maximum guaranteed number of VPN IPsec phase2 interface tunnels.	user	Not Specified	
log-disk-quota	Log disk quota in megabytes (MB). Range depends on how much disk space is available.	user	Not Specified	
name	VDOM name.	string	Maximum length: 31	
onetime-schedule	Maximum guaranteed number of firewall one-time schedules.	user	Not Specified	
proxy	Maximum guaranteed number of concurrent proxy users.	user	Not Specified	
recurring-schedule	Maximum guaranteed number of firewall recurring schedules.	user	Not Specified	
service-group	Maximum guaranteed number of firewall service groups.	user	Not Specified	
session	Maximum guaranteed number of sessions.	user	Not Specified	

Parameter	Description	Type	Size	Default
snmp-index	Permanent SNMP Index of the virtual domain.	integer	Minimum value: 1 Maximum value: 2147483647	0
sslvpn	Maximum guaranteed number of SSL-VPNs.	user	Not Specified	
user	Maximum guaranteed number of local users.	user	Not Specified	
user-group	Maximum guaranteed number of user groups.	user	Not Specified	

## config system vdom-radius-server

Configure a RADIUS server to use as a RADIUS Single Sign On (RSSO) server for this VDOM.

```
config system vdom-radius-server
    Description: Configure a RADIUS server to use as a RADIUS Single Sign On (RSSO) server
for this VDOM.
    edit <name>
        set radius-server-vdom {string}
        set status [enable|disable]
    next
end
```

## config system vdom-radius-server

Parameter	Description	Type	Size	Default
name	Name of the VDOM that you are adding the RADIUS server to.	string	Maximum length: 31	
radius-server-vdom	Use this option to select another VDOM containing a VDOM RSSO RADIUS server to use for the current VDOM.	string	Maximum length: 31	
status	Enable/disable the RSSO RADIUS server for this VDOM.	option	-	disable
		Option	Description	
		<i>enable</i>	Enable the RSSO RADIUS server for this VDOM.	
		<i>disable</i>	Disable the RSSO RADIUS server for this VDOM.	

## config system vdom-sflow

Configure sFlow per VDOM to add or change the IP address and UDP port that FortiGate sFlow agents in this VDOM use to send sFlow datagrams to an sFlow collector.

```
config system vdom-sflow
```

Description: Configure sFlow per VDOM to add or change the IP address and UDP port that FortiGate sFlow agents in this VDOM use to send sFlow datagrams to an sFlow collector.

```
set collector-ip {ipv4-address}
set collector-port {integer}
set interface {string}
set interface-select-method [auto|sdwan|...]
set source-ip {ipv4-address}
set vdom-sflow [enable|disable]
```

```
end
```

## config system vdom-sflow

Parameter	Description	Type	Size	Default								
collector-ip	IP address of the sFlow collector that sFlow agents added to interfaces in this VDOM send sFlow datagrams to.	ipv4-address	Not Specified	0.0.0.0								
collector-port	UDP port number used for sending sFlow datagrams.	integer	Minimum value: 0 Maximum value: 65535	6343								
interface	Specify outgoing interface to reach server.	string	Maximum length: 15									
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>auto</td><td>Set outgoing interface automatically.</td></tr><tr><td>sdwan</td><td>Set outgoing interface by SD-WAN or policy routing rules.</td></tr><tr><td>specify</td><td>Set outgoing interface manually.</td></tr></table>				Option	Description	auto	Set outgoing interface automatically.	sdwan	Set outgoing interface by SD-WAN or policy routing rules.	specify	Set outgoing interface manually.
Option	Description											
auto	Set outgoing interface automatically.											
sdwan	Set outgoing interface by SD-WAN or policy routing rules.											
specify	Set outgoing interface manually.											
source-ip	Source IP address for sFlow agent.	ipv4-address	Not Specified	0.0.0.0								
vdom-sflow	Enable/disable the sFlow configuration for the current VDOM.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable sFlow for this VDOM.</td></tr><tr><td>disable</td><td>Disable sFlow for this VDOM.</td></tr></table>				Option	Description	enable	Enable sFlow for this VDOM.	disable	Disable sFlow for this VDOM.		
Option	Description											
enable	Enable sFlow for this VDOM.											
disable	Disable sFlow for this VDOM.											

## config system vdom

Configure virtual domain.

```

config system vdom
  Description: Configure virtual domain.
  edit <name>
    set flag {integer}
    set short-name {string}
    set vcluster-id {integer}
  next
end

```

## config system vdom

Parameter	Description	Type	Size	Default
flag	Flag.	integer	Minimum value: 0 Maximum value: 4294967295	0
name	VDOM name.	string	Maximum length: 31	
short-name	VDOM short name.	string	Maximum length: 11	
vcluster-id	Virtual cluster ID.	integer	Minimum value: 0 Maximum value: 4294967295	0

---

## config system virtual-switch

---



This command is available for model(s): FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 140E-POE, FortiGate 140E, FortiGate 1800F, FortiGate 1801F, FortiGate 200F, FortiGate 201F, FortiGate 2600F, FortiGate 2601F, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3500F, FortiGate 3501F, FortiGate 3800D, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 600F, FortiGate 601F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 90E, FortiGate 91E, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 1000D, FortiGate 1200D, FortiGate 1500DT, FortiGate 1500D, FortiGate 2000E, FortiGate 200E, FortiGate 201E, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 3000D, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 601E, FortiGate 800D, FortiGate 900D, FortiGate VM64.

---

Configure virtual hardware switch interfaces.

```
config system virtual-switch
  Description: Configure virtual hardware switch interfaces.
  edit <name>
    set physical-switch {string}
    config port
      Description: Configure member ports.
      edit <name>
        set alias {string}
      next
    end
    set span [disable|enable]
    set span-dest-port {string}
    set span-direction [rx|tx|...]
    set span-source-port {string}
    set vlan {integer}
  next
end
```

## config system virtual-switch

Parameter	Description	Type	Size	Default								
name	Name of the virtual switch.	string	Maximum length: 15									
physical-switch	Physical switch parent.	string	Maximum length: 15									
span *	Enable/disable SPAN.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable SPAN.</td></tr><tr><td><i>enable</i></td><td>Enable SPAN.</td></tr></table>				Option	Description	<i>disable</i>	Disable SPAN.	<i>enable</i>	Enable SPAN.		
Option	Description											
<i>disable</i>	Disable SPAN.											
<i>enable</i>	Enable SPAN.											
span-dest-port *	SPAN destination port.	string	Maximum length: 15									
span-direction *	SPAN direction.	option	-	both								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>rx</i></td><td>SPAN receive direction only.</td></tr><tr><td><i>tx</i></td><td>SPAN transmit direction only.</td></tr><tr><td><i>both</i></td><td>SPAN both directions.</td></tr></table>				Option	Description	<i>rx</i>	SPAN receive direction only.	<i>tx</i>	SPAN transmit direction only.	<i>both</i>	SPAN both directions.
Option	Description											
<i>rx</i>	SPAN receive direction only.											
<i>tx</i>	SPAN transmit direction only.											
<i>both</i>	SPAN both directions.											
span-source-port *	SPAN source port.	string	Maximum length: 15									
vlan *	VLAN.	integer	Minimum value: 0 Maximum value: 4294967295	0								

\* This parameter may not exist in some models.

## config port

Parameter	Description	Type	Size	Default
name	Physical interface name.	string	Maximum length: 15	
alias	Alias.	string	Maximum length: 25	



## config system virtual-wire-pair

Configure virtual wire pairs.

```
config system virtual-wire-pair
  Description: Configure virtual wire pairs.
  edit <name>
    set member <interface-name1>, <interface-name2>, ...
    set poweroff-bypass [enable|disable]
    set poweron-bypass [enable|disable]
    set vlan-filter {user}
    set wildcard-vlan [enable|disable]
  next
end
```

## config system virtual-wire-pair

Parameter	Description	Type	Size	Default						
member <interface-name>	Interfaces belong to the virtual-wire-pair. Interface name.	string	Maximum length: 79							
name	Virtual-wire-pair name. Must be a unique interface name.	string	Maximum length: 11							
poweroff-bypass *	Enable/disable interface bypass state when power off.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable bypass when power off.</td></tr><tr><td>disable</td><td>Disable bypass when power off.</td></tr></table>	Option	Description	enable	Enable bypass when power off.	disable	Disable bypass when power off.			
Option	Description									
enable	Enable bypass when power off.									
disable	Disable bypass when power off.									
poweron-bypass *	Enable/disable interface bypass state when power on.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable bypass when power on.</td></tr><tr><td>disable</td><td>Disable bypass when power on.</td></tr></table>	Option	Description	enable	Enable bypass when power on.	disable	Disable bypass when power on.			
Option	Description									
enable	Enable bypass when power on.									
disable	Disable bypass when power on.									
vlan-filter	Set VLAN filters.	user	Not Specified							
wildcard-vlan	Enable/disable wildcard VLAN.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable wildcard VLAN.</td></tr><tr><td>disable</td><td>Disable wildcard VLAN.</td></tr></table>	Option	Description	enable	Enable wildcard VLAN.	disable	Disable wildcard VLAN.			
Option	Description									
enable	Enable wildcard VLAN.									
disable	Disable wildcard VLAN.									

\* This parameter may not exist in some models.

## config system vene-tunnel

Configure virtual network enabler tunnel.

```
config system vene-tunnel
    Description: Configure virtual network enabler tunnel.
    set auto-asic-offload [enable|disable]
    set bmr-hostname {password}
    set br {ipv6-address}
    set interface {string}
    set ipv4-address {ipv4-classnet-host}
    set mode [map-e|fixed-ip]
    set ssl-certificate {string}
    set status [enable|disable]
    set update-url {string}
end
```

## config system vene-tunnel

Parameter	Description	Type	Size	Default
auto-asic-offload *	Enable/disable tunnel ASIC offloading.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable auto ASIC offloading.		
	<i>disable</i>	Disable ASIC offloading.		
bmr-hostname	BMR hostname.	password	Not Specified	
br	Border relay IPv6 address.	ipv6-address	Not Specified	::
interface	Interface name.	string	Maximum length: 15	
ipv4-address	Tunnel IPv4 address and netmask.	ipv4-classnet-host	Not Specified	0.0.0.0 0.0.0.0
mode	VNE tunnel mode.	option	-	map-e
	<b>Option</b>	<b>Description</b>		
	<i>map-e</i>	Map-e mode.		
	<i>fixed-ip</i>	Fixed-ip mode.		
ssl-certificate	Name of local certificate for SSL connections.	string	Maximum length: 35	Fortinet_Factory

Parameter	Description	Type	Size	Default
status	Enable/disable VNE tunnel.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable VNE tunnel.		
	<i>disable</i>	Disable VNE tunnel.		
update-url	URL of provisioning server.	string	Maximum length: 511	

\* This parameter may not exist in some models.

## config system vxlan

Configure VXLAN devices.

```

config system vxlan
    Description: Configure VXLAN devices.
    edit <name>
        set dstport {integer}
        set interface {string}
        set ip-version [ipv4-unicast|ipv6-unicast|...]
        set multicast-ttl {integer}
        set remote-ip <ip1>, <ip2>, ...
        set remote-ip6 <ip61>, <ip62>, ...
        set vni {integer}
    next
end

```

## config system vxlan

Parameter	Description	Type	Size	Default				
dstport	VXLAN destination port.	integer	Minimum value: 1 Maximum value: 65535	4789				
interface	Outgoing interface for VXLAN encapsulated traffic.	string	Maximum length: 15					
ip-version	IP version to use for the VXLAN interface and so for communication over the VXLAN. IPv4 or IPv6 unicast or multicast.	option	-	ipv4-unicast				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ipv4-unicast</td><td>Use IPv4 unicast addressing over the VXLAN.</td></tr></table>				Option	Description	ipv4-unicast	Use IPv4 unicast addressing over the VXLAN.
Option	Description							
ipv4-unicast	Use IPv4 unicast addressing over the VXLAN.							

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ipv6-unicast</i></td><td>Use IPv6 unicast addressing over the VXLAN.</td></tr><tr><td><i>ipv4-multicast</i></td><td>Use IPv4 multicast addressing over the VXLAN.</td></tr><tr><td><i>ipv6-multicast</i></td><td>Use IPv6 multicast addressing over the VXLAN.</td></tr></table>	Option	Description	<i>ipv6-unicast</i>	Use IPv6 unicast addressing over the VXLAN.	<i>ipv4-multicast</i>	Use IPv4 multicast addressing over the VXLAN.	<i>ipv6-multicast</i>	Use IPv6 multicast addressing over the VXLAN.			
	Option	Description										
	<i>ipv6-unicast</i>	Use IPv6 unicast addressing over the VXLAN.										
	<i>ipv4-multicast</i>	Use IPv4 multicast addressing over the VXLAN.										
<i>ipv6-multicast</i>	Use IPv6 multicast addressing over the VXLAN.											
multicast-ttl	VXLAN multicast TTL.	integer	Minimum value: 1 Maximum value: 255	0								
name	VXLAN device or interface name. Must be a unique interface name.	string	Maximum length: 15									
remote-ip <ip>	IPv4 address of the VXLAN interface on the device at the remote end of the VXLAN. IPv4 address.	string	Maximum length: 15									
remote-ip6 <ip6>	IPv6 IP address of the VXLAN interface on the device at the remote end of the VXLAN. IPv6 address.	string	Maximum length: 45									
vni	VXLAN network ID.	integer	Minimum value: 1 Maximum value: 16777215	0								

## config system wccp

Configure WCCP.

```
config system wccp
  Description: Configure WCCP.
  edit <service-id>
    set assignment-bucket-format [wccp-v2|cisco-implementation]
    set assignment-dstaddr-mask {ipv4-netmask-any}
    set assignment-method [HASH|MASK|...]
    set assignment-srcaddr-mask {ipv4-netmask-any}
    set assignment-weight {integer}
    set authentication [enable|disable]
    set cache-engine-method [GRE|L2]
    set cache-id {ipv4-address}
    set forward-method [GRE|L2|...]
    set group-address {ipv4-address-multicast}
    set password {password}
    set ports {user}
    set ports-defined [source|destination]
    set primary-hash {option1}, {option2}, ...
    set priority {integer}
```

```

    set protocol {integer}
    set return-method [GRE|L2|...]
    set router-id {ipv4-address}
    set router-list {user}
    set server-list {user}
    set server-type [forward|proxy]
    set service-type [auto|standard|...]
next
end

```

## config system wccp

Parameter	Description	Type	Size	Default								
assignment-bucket-format	Assignment bucket format for the WCCP cache engine.	option	-	cisco-implementation								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>wccp-v2</td><td>WCCP-v2 bucket format.</td></tr><tr><td>cisco-implementation</td><td>Cisco bucket format.</td></tr></table>				Option	Description	wccp-v2	WCCP-v2 bucket format.	cisco-implementation	Cisco bucket format.		
Option	Description											
wccp-v2	WCCP-v2 bucket format.											
cisco-implementation	Cisco bucket format.											
assignment-dstaddr-mask	Assignment destination address mask.	ipv4-netmask-any	Not Specified	0.0.0.0								
assignment-method	Hash key assignment preference.	option	-	HASH								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>HASH</td><td>HASH assignment method.</td></tr><tr><td>MASK</td><td>MASK assignment method.</td></tr><tr><td>any</td><td>HASH or MASK.</td></tr></table>				Option	Description	HASH	HASH assignment method.	MASK	MASK assignment method.	any	HASH or MASK.
Option	Description											
HASH	HASH assignment method.											
MASK	MASK assignment method.											
any	HASH or MASK.											
assignment-srcaddr-mask	Assignment source address mask.	ipv4-netmask-any	Not Specified	0.0.23.65								
assignment-weight	Assignment of hash weight/ratio for the WCCP cache engine.	integer	Minimum value: 0 Maximum value: 255	0								
authentication	Enable/disable MD5 authentication.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable MD5 authentication.</td></tr><tr><td>disable</td><td>Disable MD5 authentication.</td></tr></table>				Option	Description	enable	Enable MD5 authentication.	disable	Disable MD5 authentication.		
Option	Description											
enable	Enable MD5 authentication.											
disable	Disable MD5 authentication.											

Parameter	Description	Type	Size	Default										
cache-engine-method	Method used to forward traffic to the routers or to return to the cache engine.	option	-	GRE										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>GRE</td><td>GRE encapsulation.</td></tr><tr><td>L2</td><td>L2 rewrite.</td></tr></table>	Option	Description	GRE	GRE encapsulation.	L2	L2 rewrite.							
Option	Description													
GRE	GRE encapsulation.													
L2	L2 rewrite.													
cache-id	IP address known to all routers. If the addresses are the same, use the default 0.0.0.0.	ipv4-address	Not Specified	0.0.0.0										
forward-method	Method used to forward traffic to the cache servers.	option	-	GRE										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>GRE</td><td>GRE encapsulation.</td></tr><tr><td>L2</td><td>L2 rewrite.</td></tr><tr><td>any</td><td>GRE or L2.</td></tr></table>	Option	Description	GRE	GRE encapsulation.	L2	L2 rewrite.	any	GRE or L2.					
Option	Description													
GRE	GRE encapsulation.													
L2	L2 rewrite.													
any	GRE or L2.													
group-address	IP multicast address used by the cache routers. For the FortiGate to ignore multicast WCCP traffic, use the default 0.0.0.0.	ipv4-address-multicast	Not Specified	0.0.0.0										
password	Password for MD5 authentication.	password	Not Specified											
ports	Service ports.	user	Not Specified											
ports-defined	Match method.	option	-											
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>source</td><td>Source port match.</td></tr><tr><td>destination</td><td>Destination port match.</td></tr></table>	Option	Description	source	Source port match.	destination	Destination port match.							
Option	Description													
source	Source port match.													
destination	Destination port match.													
primary-hash	Hash method.	option	-	dst-ip										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>src-ip</td><td>Source IP hash.</td></tr><tr><td>dst-ip</td><td>Destination IP hash.</td></tr><tr><td>src-port</td><td>Source port hash.</td></tr><tr><td>dst-port</td><td>Destination port hash.</td></tr></table>	Option	Description	src-ip	Source IP hash.	dst-ip	Destination IP hash.	src-port	Source port hash.	dst-port	Destination port hash.			
Option	Description													
src-ip	Source IP hash.													
dst-ip	Destination IP hash.													
src-port	Source port hash.													
dst-port	Destination port hash.													

Parameter	Description	Type	Size	Default
priority	Service priority.	integer	Minimum value: 0 Maximum value: 255	0
protocol	Service protocol.	integer	Minimum value: 0 Maximum value: 255	0
return-method	Method used to decline a redirected packet and return it to the FortiGate unit.	option	-	GRE
	OptionDescription			
	GRE	GRE encapsulation.		
	L2	L2 rewrite.		
	any	GRE or L2.		
router-id	IP address known to all cache engines. If all cache engines connect to the same FortiGate interface, use the default 0.0.0.0.	ipv4-address	Not Specified	0.0.0.0
router-list	IP addresses of one or more WCCP routers.	user	Not Specified	
server-list	IP addresses and netmasks for up to four cache servers.	user	Not Specified	
server-type	Cache server type.	option	-	forward
	OptionDescription			
	forward	Forward server.		
	proxy	Proxy server.		
service-id	Service ID.	string	Maximum length: 3	
service-type	WCCP service type used by the cache server for logical interception and redirection of traffic.	option	-	auto
	OptionDescription			
	auto	auto		
	standard	Standard service.		
	dynamic	Dynamic service.		

## config system wireless ap-status



This command is available for model(s): FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F.

It is not available for: FortiGate 1000D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

Configure accepted wireless AP.

```
config system wireless ap-status
    Description: Configure accepted wireless AP.
    edit <id>
        set bssid {mac-address}
        set ssid {string}
        set status [rogue|accepted|...]
    next
end
```

## config system wireless ap-status

Parameter	Description	Type	Size	Default
bssid	AP's BSSID.	mac-address	Not Specified	00:00:00:00:00:00
id	AP ID.	integer	Minimum value: 0 Maximum value: 4294967295	0



Parameter	Description	Type	Size	Default
ssid	AP's ssid	string	Maximum length: 32	
status	AP status.	option	-	rogue
	<div><div>Option</div><div>Description</div></div>			
	<i>rogue</i>	Rogue.		
	<i>accepted</i>	Accepted.		
	<i>suppressed</i>	Suppressed.		

## config system wireless settings



This command is available for model(s): FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 61E, FortiWiFi 61F.

It is not available for: FortiGate 1000D, FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 101E, FortiGate 101F, FortiGate 1100E, FortiGate 1101E, FortiGate 1200D, FortiGate 140E-POE, FortiGate 140E, FortiGate 1500DT, FortiGate 1500D, FortiGate 1800F, FortiGate 1801F, FortiGate 2000E, FortiGate 200E, FortiGate 200F, FortiGate 201E, FortiGate 201F, FortiGate 2200E, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3000F, FortiGate 3001F, FortiGate 300E, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3300E, FortiGate 3301E, FortiGate 3400E, FortiGate 3401E, FortiGate 3500F, FortiGate 3501F, FortiGate 3600E, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 401E, FortiGate 401F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4201F, FortiGate 4400F, FortiGate 4401F, FortiGate 5001E1, FortiGate 5001E, FortiGate 500E, FortiGate 501E, FortiGate 600E, FortiGate 600F, FortiGate 601E, FortiGate 601F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 61E, FortiGate 61F, FortiGate 70F, FortiGate 71F, FortiGate 800D, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 90E, FortiGate 91E, FortiGate VM64, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 80F 2R, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

### Wireless radio configuration.

```
config system wireless settings
    Description: Wireless radio configuration.
    set band [802.11a|802.11b|...]
    set beacon-interval {integer}
    set bgscan [disable|enable]
    set bgscan-idle {integer}
    set bgscan-interval {integer}
    set channel {integer}
    set channel-bonding [enable|disable]
    set geography [World|Americas|...]
```

```

set mode [CLIENT|AP|...]
set power-level {integer}
set rogue-scan [enable|disable]
set rogue-scan-mac-adjacency {integer}
set short-guard-interval [enable|disable]

```

end

## config system wireless settings

Parameter	Description	Type	Size	Default
band	Band.	option	-	802.11g
	<div>OptionDescription</div>			
	802.11a	802.11a.		
	802.11b	802.11b.		
	802.11g	802.11g.		
	802.11g-only	802.11g only.		
	802.11n	802.11n at 2.4G band.		
	802.11ng-only	802.11ng only at 2.4G band.		
	802.11n-only	802.11n only at 2.4G band.		
	802.11n-5G	802.11n at 5G band.		
	802.11n-5G-only	802.11n only at 5G band.		
	802.11ac	802.11ac at 5G band.		
	802.11acn-only	802.11acn only at 5G band.		
	802.11ac-only	802.11ac only at 5G band.		
	beacon-interval	Beacon level.	integer	Minimum value: 25 Maximum value: 1000
bgscan	Enable/disable background rogue AP scan.	option	-	disable
	<div>OptionDescription</div>			
	disable	Disable background rogue AP scan.		
	enable	Enable background rogue AP scan.		
bgscan-idle	Interval between scanning channels.	integer	Minimum value: 100 Maximum value: 1000	250

Parameter	Description	Type	Size	Default
bgscan-interval	Interval between two rounds of scanning.	integer	Minimum value: 15 Maximum value: 3600	120
channel	Channel.	integer	Minimum value: 0 Maximum value: 4294967295	0
channel-bonding	Supported channel width.	option	-	disable
	OptionDescription			
	enable	20/40 MHz.		
	disable	20 MHz.		
geography	Geography.	option	-	Americas
	OptionDescription			
	World	World.		
	Americas	Americas.		
	EMEA	EMEA.		
	Israel	Israel.		
	Japan	Japan.		
mode	Mode.	option	-	AP
	OptionDescription			
	CLIENT	Client.		
	AP	Access point.		
	SCAN	Scan.		
power-level	Power level.	integer	Minimum value: 0 Maximum value: 17	17
rogue-scan	Enable/disable rogue scan.	option	-	disable

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable rogue scan.		
	<i>disable</i>	Disable rogue scan.		
rogue-scan-mac-adjacency	MAC adjacency.	integer	Minimum value: 0 Maximum value: 31	7
short-guard-interval	Enable/disable short guard interval.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	400 ns long guard interval.		
	<i>disable</i>	800 ns short guard interval.		

## config system zone

Configure zones to group two or more interfaces. When a zone is created you can configure policies for the zone instead of individual interfaces in the zone.

```
config system zone
    Description: Configure zones to group two or more interfaces. When a zone is created you
    can configure policies for the zone instead of individual interfaces in the zone.
    edit <name>
        set description {string}
        set interface <interface-name1>, <interface-name2>, ...
        set intrazone [allow|deny]
        config tagging
            Description: Config object tagging.
            edit <name>
                set category {string}
                set tags <name1>, <name2>, ...
            next
        end
    next
end
```

## config system zone

Parameter	Description	Type	Size	Default
description	Description.	string	Maximum length: 127	

Parameter	Description	Type	Size	Default						
interface <interface-name>	Add interfaces to this zone. Interfaces must not be assigned to another zone or have firewall policies defined. Select interfaces to add to the zone.	string	Maximum length: 79							
intrazone	Allow or deny traffic routing between different interfaces in the same zone.	option	-	deny						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allow traffic between interfaces in the zone.</td></tr><tr><td>deny</td><td>Deny traffic between interfaces in the zone.</td></tr></table>				Option	Description	allow	Allow traffic between interfaces in the zone.	deny	Deny traffic between interfaces in the zone.
Option	Description									
allow	Allow traffic between interfaces in the zone.									
deny	Deny traffic between interfaces in the zone.									
name	Zone name.	string	Maximum length: 35							

### config tagging

Parameter	Description	Type	Size	Default
name	Tagging entry name.	string	Maximum length: 63	
category	Tag category.	string	Maximum length: 63	
tags <name>	Tags. Tag name.	string	Maximum length: 79	

## user

This section includes syntax for the following commands:

- [config user adgrp on page 1570](#)
- [config user certificate on page 1571](#)
- [config user domain-controller on page 1572](#)
- [config user exchange on page 1575](#)
- [config user fortitoken on page 1577](#)
- [config user fsso-polling on page 1578](#)
- [config user fsso on page 1580](#)
- [config user group on page 1584](#)
- [config user krb-keytab on page 1589](#)
- [config user ldap on page 1590](#)
- [config user local on page 1596](#)
- [config user nac-policy on page 1599](#)
- [config user password-policy on page 1601](#)
- [config user peer on page 1602](#)
- [config user peergrp on page 1604](#)
- [config user pop3 on page 1604](#)
- [config user quarantine on page 1605](#)
- [config user radius on page 1607](#)
- [config user saml on page 1618](#)
- [config user security-exempt-list on page 1622](#)
- [config user setting on page 1623](#)
- [config user tacacs+ on page 1627](#)

### config user adgrp

Configure FSSO groups.

```
config user adgrp
    Description: Configure FSSO groups.
    edit <name>
        set connector-source {string}
        set id {integer}
        set server-name {string}
    next
end
```

## config user adgrp

Parameter	Description	Type	Size	Default
connector-source	FSSO connector source.	string	Maximum length: 35	
id	Group ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
name	Name.	string	Maximum length: 511	
server-name	FSSO agent name.	string	Maximum length: 35	

## config user certificate

Configure certificate users.

```
config user certificate
  Description: Configure certificate users.
  edit <name>
    set common-name {string}
    set id {integer}
    set issuer {string}
    set status [enable|disable]
    set type [single-certificate|trusted-issuer]
  next
end
```

## config user certificate

Parameter	Description	Type	Size	Default
common-name	Certificate common name.	string	Maximum length: 64	
id	User ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
issuer	CA certificate used for client certificate verification.	string	Maximum length: 79	

Parameter	Description	Type	Size	Default
name	User name.	string	Maximum length: 64	
status	Enable/disable allowing the certificate user to authenticate with the FortiGate unit.	option	-	enable
		Option	Description	
		<i>enable</i>	Enable user.	
		<i>disable</i>	Disable user.	
type	Type of certificate authentication method.	option	-	single-certificate
		Option	Description	
		<i>single-certificate</i>	Single certificate.	
		<i>trusted-issuer</i>	Trusted CA issuer.	

## config user domain-controller

Configure domain controller entries.

```

config user domain-controller
    Description: Configure domain controller entries.
    edit <name>
        set ad-mode [none|ds|...]
        set adlds-dn {string}
        set adlds-ip-address {ipv4-address}
        set adlds-ip6 {ipv6-address}
        set adlds-port {integer}
        set dns-srv-lookup [enable|disable]
        set domain-name {string}
        config extra-server
            Description: Extra servers.
            edit <id>
                set ip-address {ipv4-address}
                set port {integer}
                set source-ip-address {ipv4-address}
                set source-port {integer}
            next
        end
        set hostname {string}
        set interface {string}
        set interface-select-method [auto|sdwan|...]
        set ip-address {ipv4-address}
        set ip6 {ipv6-address}
        set ldap-server <name1>, <name2>, ...
        set password {password}
        set port {integer}
        set replication-port {integer}
    
```



```

        set source-ip-address {ipv4-address}
        set source-ip6 {ipv6-address}
        set source-port {integer}
        set username {string}
    next
end

```

## config user domain-controller

Parameter	Description	Type	Size	Default
ad-mode	Set Active Directory mode.	option	-	none
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	The server is not configured as an Active Directory Domain Server (AD DS).		
	<i>ds</i>	The server is configured as an Active Directory Domain Server (AD DS).		
	<i>lds</i>	The server is an Active Directory Lightweight Domain Server (AD LDS).		
adlds-dn	AD LDS distinguished name.	string	Maximum length: 255	
adlds-ip-address	AD LDS IPv4 address.	ipv4-address	Not Specified	0.0.0.0
adlds-ip6	AD LDS IPv6 address.	ipv6-address	Not Specified	::
adlds-port	Port number of AD LDS service.	integer	Minimum value: 0 Maximum value: 65535	389
dns-srv-lookup	Enable/disable DNS service lookup.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable DNS service lookup.		
	<i>disable</i>	Disable DNS service lookup.		
domain-name	Domain DNS name.	string	Maximum length: 255	
hostname	Hostname of the server to connect to.	string	Maximum length: 255	
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	

Parameter	Description	Type	Size	Default								
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>auto</td><td>Set outgoing interface automatically.</td></tr><tr><td>sdwan</td><td>Set outgoing interface by SD-WAN or policy routing rules.</td></tr><tr><td>specify</td><td>Set outgoing interface manually.</td></tr></table>	Option	Description	auto	Set outgoing interface automatically.	sdwan	Set outgoing interface by SD-WAN or policy routing rules.	specify	Set outgoing interface manually.			
	Option	Description										
	auto	Set outgoing interface automatically.										
	sdwan	Set outgoing interface by SD-WAN or policy routing rules.										
specify	Set outgoing interface manually.											
ip-address	Domain controller IPv4 address.	ipv4-address	Not Specified	0.0.0.0								
ip6	Domain controller IPv6 address.	ipv6-address	Not Specified	::								
ldap-server<name>	LDAP server name(s). LDAP server name.	string	Maximum length: 79									
name	Domain controller entry name.	string	Maximum length: 35									
password	Password for specified username.	password	Not Specified									
port	Port to be used for communication with the domain controller.	integer	Minimum value: 0 Maximum value: 65535	445								
replication-port	Port to be used for communication with the domain controller for replication service. Port number 0 indicates automatic discovery.	integer	Minimum value: 0 Maximum value: 65535	0								
source-ip-address	FortiGate IPv4 address to be used for communication with the domain controller.	ipv4-address	Not Specified	0.0.0.0								
source-ip6	FortiGate IPv6 address to be used for communication with the domain controller.	ipv6-address	Not Specified	::								
source-port	Source port to be used for communication with the domain controller.	integer	Minimum value: 0 Maximum value: 65535	0								
username	User name to sign in with. Must have proper permissions for service.	string	Maximum length: 64									

## config extra-server

Parameter	Description	Type	Size	Default
id	Server ID.	integer	Minimum value: 1 Maximum value: 100	0
ip-address	Domain controller IP address.	ipv4-address	Not Specified	0.0.0.0
port	Port to be used for communication with the domain controller.	integer	Minimum value: 0 Maximum value: 65535	445
source-ip-address	FortiGate IPv4 address to be used for communication with the domain controller.	ipv4-address	Not Specified	0.0.0.0
source-port	Source port to be used for communication with the domain controller.	integer	Minimum value: 0 Maximum value: 65535	0

## config user exchange

Configure MS Exchange server entries.

```
config user exchange
  Description: Configure MS Exchange server entries.
  edit <name>
    set auth-level [connect|call|...]
    set auth-type [spnego|ntlm|...]
    set auto-discover-kdc [enable|disable]
    set connect-protocol [rpc-over-tcp|rpc-over-http|...]
    set domain-name {string}
    set http-auth-type [basic|ntlm]
    set ip {ipv4-address-any}
    set kdc-ip <ipv41>, <ipv42>, ...
    set password {password}
    set server-name {string}
    set ssl-min-proto-version [default|SSLv3|...]
    set username {string}
  next
end
```

## config user exchange

Parameter	Description	Type	Size	Default												
auth-level	Authentication security level used for the RPC protocol layer.	option	-	privacy												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>connect</i></td><td>RPC authentication level 'connect'.</td></tr><tr><td><i>call</i></td><td>RPC authentication level 'call'.</td></tr><tr><td><i>packet</i></td><td>RPC authentication level 'packet'.</td></tr><tr><td><i>integrity</i></td><td>RPC authentication level 'integrity'.</td></tr><tr><td><i>privacy</i></td><td>RPC authentication level 'privacy'.</td></tr></table>	Option	Description	<i>connect</i>	RPC authentication level 'connect'.	<i>call</i>	RPC authentication level 'call'.	<i>packet</i>	RPC authentication level 'packet'.	<i>integrity</i>	RPC authentication level 'integrity'.	<i>privacy</i>	RPC authentication level 'privacy'.			
Option	Description															
<i>connect</i>	RPC authentication level 'connect'.															
<i>call</i>	RPC authentication level 'call'.															
<i>packet</i>	RPC authentication level 'packet'.															
<i>integrity</i>	RPC authentication level 'integrity'.															
<i>privacy</i>	RPC authentication level 'privacy'.															
auth-type	Authentication security type used for the RPC protocol layer.	option	-	kerberos												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>spnego</i></td><td>Negotiate authentication.</td></tr><tr><td><i>ntlm</i></td><td>NTLM authentication.</td></tr><tr><td><i>kerberos</i></td><td>Kerberos authentication.</td></tr></table>	Option	Description	<i>spnego</i>	Negotiate authentication.	<i>ntlm</i>	NTLM authentication.	<i>kerberos</i>	Kerberos authentication.							
Option	Description															
<i>spnego</i>	Negotiate authentication.															
<i>ntlm</i>	NTLM authentication.															
<i>kerberos</i>	Kerberos authentication.															
auto-discover-kdc	Enable/disable automatic discovery of KDC IP addresses.	option	-	enable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable automatic discovery of KDC IP addresses.</td></tr><tr><td><i>disable</i></td><td>Disable automatic discovery of KDC IP addresses.</td></tr></table>	Option	Description	<i>enable</i>	Enable automatic discovery of KDC IP addresses.	<i>disable</i>	Disable automatic discovery of KDC IP addresses.									
Option	Description															
<i>enable</i>	Enable automatic discovery of KDC IP addresses.															
<i>disable</i>	Disable automatic discovery of KDC IP addresses.															
connect-protocol	Connection protocol used to connect to MS Exchange service.	option	-	rpc-over-https												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>rpc-over-tcp</i></td><td>Connect using RPC-over-TCP. Use for MS Exchange 2010 and earlier versions. Supported in MS Exchange 2013.</td></tr><tr><td><i>rpc-over-http</i></td><td>Connect using RPC-over-HTTP. Use for MS Exchange 2016 and later versions. Supported in MS Exchange 2013.</td></tr><tr><td><i>rpc-over-https</i></td><td>Connect using RPC-over-HTTPS. Use for MS Exchange 2016 and later versions. Supported in MS Exchange 2013.</td></tr></table>	Option	Description	<i>rpc-over-tcp</i>	Connect using RPC-over-TCP. Use for MS Exchange 2010 and earlier versions. Supported in MS Exchange 2013.	<i>rpc-over-http</i>	Connect using RPC-over-HTTP. Use for MS Exchange 2016 and later versions. Supported in MS Exchange 2013.	<i>rpc-over-https</i>	Connect using RPC-over-HTTPS. Use for MS Exchange 2016 and later versions. Supported in MS Exchange 2013.							
Option	Description															
<i>rpc-over-tcp</i>	Connect using RPC-over-TCP. Use for MS Exchange 2010 and earlier versions. Supported in MS Exchange 2013.															
<i>rpc-over-http</i>	Connect using RPC-over-HTTP. Use for MS Exchange 2016 and later versions. Supported in MS Exchange 2013.															
<i>rpc-over-https</i>	Connect using RPC-over-HTTPS. Use for MS Exchange 2016 and later versions. Supported in MS Exchange 2013.															
domain-name	MS Exchange server fully qualified domain name.	string	Maximum length: 79													

Parameter	Description	Type	Size	Default												
http-auth-type	Authentication security type used for the HTTP transport.	option	-	ntlm												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>basic</i></td><td>Basic HTTP authentication.</td></tr><tr><td><i>ntlm</i></td><td>NTLM HTTP authentication.</td></tr></table>	Option	Description	<i>basic</i>	Basic HTTP authentication.	<i>ntlm</i>	NTLM HTTP authentication.									
	Option	Description														
	<i>basic</i>	Basic HTTP authentication.														
<i>ntlm</i>	NTLM HTTP authentication.															
ip	Server IPv4 address.	ipv4-address-any	Not Specified	0.0.0.0												
kdc-ip <ipv4>	KDC IPv4 addresses for Kerberos authentication. KDC IPv4 addresses for Kerberos authentication.	string	Maximum length: 79													
name	MS Exchange server entry name.	string	Maximum length: 35													
password	Password for the specified username.	password	Not Specified													
server-name	MS Exchange server hostname.	string	Maximum length: 63													
ssl-min-protocol-version	Minimum SSL/TLS protocol version for HTTPS transport.	option	-	default												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>Follow system global setting.</td></tr><tr><td><i>SSLv3</i></td><td>SSLv3.</td></tr><tr><td><i>TLSv1</i></td><td>TLSv1.</td></tr><tr><td><i>TLSv1-1</i></td><td>TLSv1.1.</td></tr><tr><td><i>TLSv1-2</i></td><td>TLSv1.2.</td></tr></table>	Option	Description	<i>default</i>	Follow system global setting.	<i>SSLv3</i>	SSLv3.	<i>TLSv1</i>	TLSv1.	<i>TLSv1-1</i>	TLSv1.1.	<i>TLSv1-2</i>	TLSv1.2.			
	Option	Description														
	<i>default</i>	Follow system global setting.														
	<i>SSLv3</i>	SSLv3.														
	<i>TLSv1</i>	TLSv1.														
	<i>TLSv1-1</i>	TLSv1.1.														
<i>TLSv1-2</i>	TLSv1.2.															
username	User name used to sign in to the server. Must have proper permissions for service.	string	Maximum length: 64													

## config user fortitoken

Configure FortiToken.

```
config user fortitoken
    Description: Configure FortiToken.
    edit <serial-number>
        set activation-code {string}
        set activation-expire {integer}
        set comments {var-string}
        set license {string}
```

```

        set os-ver {string}
        set reg-id {string}
        set seed {string}
        set status [active|lock]
    next
end

```

## config user fortitoken

Parameter	Description	Type	Size	Default
activation-code	Mobile token user activation-code.	string	Maximum length: 32	
activation-expire	Mobile token user activation-code expire time.	integer	Minimum value: 0 Maximum value: 4294967295	0
comments	Comment.	var-string	Maximum length: 255	
license	Mobile token license.	string	Maximum length: 31	
os-ver	Device Mobile Version.	string	Maximum length: 15	
reg-id	Device Reg ID.	string	Maximum length: 256	
seed	Token seed.	string	Maximum length: 200	
serial-number	Serial number.	string	Maximum length: 16	
status	Status.	option	-	active
		Option	Description	
		<i>active</i>	Activate FortiToken.	
		<i>lock</i>	Lock FortiToken.	

## config user fsso-polling

Configure FSSO active directory servers for polling mode.

```

config user fsso-polling
    Description: Configure FSSO active directory servers for polling mode.
    edit <id>
        config adgrp

```

```

        Description: LDAP Group Info.
        edit <name>
        next
    end
    set default-domain {string}
    set ldap-server {string}
    set logon-history {integer}
    set password {password}
    set polling-frequency {integer}
    set port {integer}
    set server {string}
    set smb-ntlmv1-auth [enable|disable]
    set smbv1 [enable|disable]
    set status [enable|disable]
    set user {string}
next
end

```

### config user fsso-polling

Parameter	Description	Type	Size	Default
default-domain	Default domain managed by this Active Directory server.	string	Maximum length: 35	
id	Active Directory server ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
ldap-server	LDAP server name used in LDAP connection strings.	string	Maximum length: 35	
logon-history	Number of hours of logon history to keep, 0 means keep all history.	integer	Minimum value: 0 Maximum value: 48	8
password	Password required to log into this Active Directory server.	password	Not Specified	
polling-frequency	Polling frequency (every 1 to 30 seconds).	integer	Minimum value: 1 Maximum value: 30	10
port	Port to communicate with this Active Directory server.	integer	Minimum value: 0 Maximum value: 65535	0

Parameter	Description	Type	Size	Default						
server	Host name or IP address of the Active Directory server.	string	Maximum length: 63							
smb-ntlmv1-auth	Enable/disable support of NTLMv1 for Samba authentication.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable support of NTLMv1 for Samba authentication.</td></tr><tr><td><i>disable</i></td><td>Disable support of NTLMv1 for Samba authentication.</td></tr></table>	Option	Description	<i>enable</i>	Enable support of NTLMv1 for Samba authentication.	<i>disable</i>	Disable support of NTLMv1 for Samba authentication.			
Option	Description									
<i>enable</i>	Enable support of NTLMv1 for Samba authentication.									
<i>disable</i>	Disable support of NTLMv1 for Samba authentication.									
smbv1	Enable/disable support of SMBv1 for Samba.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable support of SMBv1 for Samba.</td></tr><tr><td><i>disable</i></td><td>Disable support of SMBv1 for Samba.</td></tr></table>	Option	Description	<i>enable</i>	Enable support of SMBv1 for Samba.	<i>disable</i>	Disable support of SMBv1 for Samba.			
Option	Description									
<i>enable</i>	Enable support of SMBv1 for Samba.									
<i>disable</i>	Disable support of SMBv1 for Samba.									
status	Enable/disable polling for the status of this Active Directory server.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
user	User name required to log into this Active Directory server.	string	Maximum length: 35							

## config adgrp

Parameter	Description	Type	Size	Default
name	Name.	string	Maximum length: 511	

## config user fsso

Configure Fortinet Single Sign On (FSSO) agents.

```
config user fsso
  Description: Configure Fortinet Single Sign On (FSSO) agents.
  edit <name>
    set group-poll-interval {integer}
    set interface {string}
    set interface-select-method [auto|sdwan|...]
    set ldap-poll [enable|disable]
    set ldap-poll-filter {string}
    set ldap-poll-interval {integer}
```



```

set ldap-server {string}
set logon-timeout {integer}
set password {password}
set password2 {password}
set password3 {password}
set password4 {password}
set password5 {password}
set port {integer}
set port2 {integer}
set port3 {integer}
set port4 {integer}
set port5 {integer}
set server {string}
set server2 {string}
set server3 {string}
set server4 {string}
set server5 {string}
set source-ip {ipv4-address}
set source-ip6 {ipv6-address}
set ssl [enable|disable]
set ssl-server-host-ip-check [enable|disable]
set ssl-trusted-cert {string}
set type [default|fortinac]
set user-info-server {string}
next
end

```

## config user fsso

Parameter	Description	Type	Size	Default
group-poll-interval	Interval in minutes within to fetch groups from FSSO server, or unset to disable.	integer	Minimum value: 1 Maximum value: 2880	0
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto
	Option	Description		
	auto	Set outgoing interface automatically.		
	sdwan	Set outgoing interface by SD-WAN or policy routing rules.		
	specify	Set outgoing interface manually.		
ldap-poll	Enable/disable automatic fetching of groups from LDAP server.	option	-	disable

Parameter	Description	Type	Size	Default
	Option	Description		
	enable	Enable automatic fetching of groups from LDAP server.		
	disable	Disable automatic fetching of groups from LDAP server.		
ldap-poll-filter	Filter used to fetch groups.	string	Maximum length: 2047	(objectCategory=group)
ldap-poll-interval	Interval in minutes within to fetch groups from LDAP server.	integer	Minimum value: 1 Maximum value: 2880	180
ldap-server	LDAP server to get group information.	string	Maximum length: 35	
logon-timeout	Interval in minutes to keep logons after FSSO server down.	integer	Minimum value: 1 Maximum value: 2880	5
name	Name.	string	Maximum length: 35	
password	Password of the first FSSO collector agent.	password	Not Specified	
password2	Password of the second FSSO collector agent.	password	Not Specified	
password3	Password of the third FSSO collector agent.	password	Not Specified	
password4	Password of the fourth FSSO collector agent.	password	Not Specified	
password5	Password of the fifth FSSO collector agent.	password	Not Specified	
port	Port of the first FSSO collector agent.	integer	Minimum value: 1 Maximum value: 65535	8000
port2	Port of the second FSSO collector agent.	integer	Minimum value: 1 Maximum value: 65535	8000

Parameter	Description	Type	Size	Default						
port3	Port of the third FSSO collector agent.	integer	Minimum value: 1 Maximum value: 65535	8000						
port4	Port of the fourth FSSO collector agent.	integer	Minimum value: 1 Maximum value: 65535	8000						
port5	Port of the fifth FSSO collector agent.	integer	Minimum value: 1 Maximum value: 65535	8000						
server	Domain name or IP address of the first FSSO collector agent.	string	Maximum length: 63							
server2	Domain name or IP address of the second FSSO collector agent.	string	Maximum length: 63							
server3	Domain name or IP address of the third FSSO collector agent.	string	Maximum length: 63							
server4	Domain name or IP address of the fourth FSSO collector agent.	string	Maximum length: 63							
server5	Domain name or IP address of the fifth FSSO collector agent.	string	Maximum length: 63							
source-ip	Source IP for communications to FSSO agent.	ipv4-address	Not Specified	0.0.0.0						
source-ip6	IPv6 source for communications to FSSO agent.	ipv6-address	Not Specified	::						
ssl	Enable/disable use of SSL.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable use of SSL.</td></tr><tr><td><i>disable</i></td><td>Disable use of SSL.</td></tr></table>				Option	Description	<i>enable</i>	Enable use of SSL.	<i>disable</i>	Disable use of SSL.
Option	Description									
<i>enable</i>	Enable use of SSL.									
<i>disable</i>	Disable use of SSL.									
ssl-server-host-ip-check	Enable/disable server host/IP verification.	option	-	disable						

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable server host/IP verification.		
	<i>disable</i>	Disable server host/IP verification.		
ssl-trusted-cert	Trusted server certificate or CA certificate.	string	Maximum length: 79	
type	Server type.	option	-	default
	<b>Option</b>	<b>Description</b>		
	<i>default</i>	All other unspecified types of servers.		
	<i>fortinac</i>	FortiNAC server.		
user-info-server	LDAP server to get user information.	string	Maximum length: 35	

## config user group

Configure user groups.

```

config user group
  Description: Configure user groups.
  edit <name>
    set auth-concurrent-override [enable|disable]
    set auth-concurrent-value {integer}
    set authtimeout {integer}
    set company [optional|mandatory|...]
    set email [disable|enable]
    set expire {integer}
    set expire-type [immediately|first-successful-login]
    set group-type [firewall|fsso-service|...]
    config guest
      Description: Guest User.
      edit <id>
        set user-id {string}
        set name {string}
        set password {password}
        set mobile-phone {string}
        set sponsor {string}
        set company {string}
        set email {string}
        set expiration {user}
        set comment {var-string}
      next
    end
    set http-digest-realm {string}
    set id {integer}
  config match
    Description: Group matches.

```

```

        edit <id>
            set server-name {string}
            set group-name {string}
        next
    end
    set max-accounts {integer}
    set member <name1>, <name2>, ...
    set mobile-phone [disable|enable]
    set multiple-guest-add [disable|enable]
    set password [auto-generate|specify|...]
    set sms-custom-server {string}
    set sms-server [fortiguard|custom]
    set sponsor [optional|mandatory|...]
    set sso-attribute-value {string}
    set user-id [email|auto-generate|...]
    set user-name [disable|enable]
next
end

```

## config user group

Parameter	Description	Type	Size	Default								
auth-concurrent-override	Enable/disable overriding the global number of concurrent authentication sessions for this user group.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable auth-concurrent-override.</td></tr><tr><td><i>disable</i></td><td>Disable auth-concurrent-override.</td></tr></table>	Option	Description	<i>enable</i>	Enable auth-concurrent-override.	<i>disable</i>	Disable auth-concurrent-override.					
Option	Description											
<i>enable</i>	Enable auth-concurrent-override.											
<i>disable</i>	Disable auth-concurrent-override.											
auth-concurrent-value	Maximum number of concurrent authenticated connections per user.	integer	Minimum value: 0 Maximum value: 100	0								
authtimeout	Authentication timeout in minutes for this user group. 0 to use the global user setting auth-timeout.	integer	Minimum value: 0 Maximum value: 43200	0								
company	Set the action for the company guest user field.	option	-	optional								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>optional</i></td><td>Optional.</td></tr><tr><td><i>mandatory</i></td><td>Mandatory.</td></tr><tr><td><i>disabled</i></td><td>Disabled.</td></tr></table>	Option	Description	<i>optional</i>	Optional.	<i>mandatory</i>	Mandatory.	<i>disabled</i>	Disabled.			
Option	Description											
<i>optional</i>	Optional.											
<i>mandatory</i>	Mandatory.											
<i>disabled</i>	Disabled.											
email	Enable/disable the guest user email address field.	option	-	enable								

Parameter	Description	Type	Size	Default										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Enable setting.</td></tr><tr><td><i>enable</i></td><td>Disable setting.</td></tr></table>				Option	Description	<i>disable</i>	Enable setting.	<i>enable</i>	Disable setting.				
	Option	Description												
	<i>disable</i>	Enable setting.												
<i>enable</i>	Disable setting.													
expire	Time in seconds before guest user accounts expire.	integer	Minimum value: 1 Maximum value: 31536000	14400										
expire-type	Determine when the expiration countdown begins.	option	-	immediately										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>immediately</i></td><td>Immediately.</td></tr><tr><td><i>first-successful-login</i></td><td>First successful login.</td></tr></table>				Option	Description	<i>immediately</i>	Immediately.	<i>first-successful-login</i>	First successful login.				
	Option	Description												
	<i>immediately</i>	Immediately.												
<i>first-successful-login</i>	First successful login.													
group-type	Set the group to be for firewall authentication, FSSO, RSSO, or guest users.	option	-	firewall										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>firewall</i></td><td>Firewall.</td></tr><tr><td><i>fsso-service</i></td><td>Fortinet Single Sign-On Service.</td></tr><tr><td><i>rsso</i></td><td>RADIUS based Single Sign-On Service.</td></tr><tr><td><i>guest</i></td><td>Guest.</td></tr></table>				Option	Description	<i>firewall</i>	Firewall.	<i>fsso-service</i>	Fortinet Single Sign-On Service.	<i>rsso</i>	RADIUS based Single Sign-On Service.	<i>guest</i>	Guest.
	Option	Description												
	<i>firewall</i>	Firewall.												
	<i>fsso-service</i>	Fortinet Single Sign-On Service.												
	<i>rsso</i>	RADIUS based Single Sign-On Service.												
<i>guest</i>	Guest.													
http-digest-realm	Realm attribute for MD5-digest authentication.	string	Maximum length: 35											
id	Group ID.	integer	Minimum value: 0 Maximum value: 4294967295	0										
max-accounts	Maximum number of guest accounts that can be created for this group (0 means unlimited).	integer	Minimum value: 0 Maximum value: 1024 **	0										
member <name>	Names of users, peers, LDAP servers, or RADIUS servers to add to the user group. Group member name.	string	Maximum length: 511											

Parameter	Description	Type	Size	Default								
mobile-phone	Enable/disable the guest user mobile phone number field.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Enable setting.</td></tr><tr><td><i>enable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>disable</i>	Enable setting.	<i>enable</i>	Disable setting.					
Option	Description											
<i>disable</i>	Enable setting.											
<i>enable</i>	Disable setting.											
multiple-guest-add	Enable/disable addition of multiple guests.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Enable setting.</td></tr><tr><td><i>enable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>disable</i>	Enable setting.	<i>enable</i>	Disable setting.					
Option	Description											
<i>disable</i>	Enable setting.											
<i>enable</i>	Disable setting.											
name	Group name.	string	Maximum length: 35									
password	Guest user password type.	option	-	auto-generate								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto-generate</i></td><td>Automatically generate.</td></tr><tr><td><i>specify</i></td><td>Specify.</td></tr><tr><td><i>disable</i></td><td>Disable.</td></tr></table>	Option	Description	<i>auto-generate</i>	Automatically generate.	<i>specify</i>	Specify.	<i>disable</i>	Disable.			
Option	Description											
<i>auto-generate</i>	Automatically generate.											
<i>specify</i>	Specify.											
<i>disable</i>	Disable.											
sms-custom-server	SMS server.	string	Maximum length: 35									
sms-server	Send SMS through FortiGuard or other external server.	option	-	fortiguard								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>fortiguard</i></td><td>Send SMS by FortiGuard.</td></tr><tr><td><i>custom</i></td><td>Send SMS by custom server.</td></tr></table>	Option	Description	<i>fortiguard</i>	Send SMS by FortiGuard.	<i>custom</i>	Send SMS by custom server.					
Option	Description											
<i>fortiguard</i>	Send SMS by FortiGuard.											
<i>custom</i>	Send SMS by custom server.											
sponsor	Set the action for the sponsor guest user field.	option	-	optional								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>optional</i></td><td>Optional.</td></tr><tr><td><i>mandatory</i></td><td>Mandatory.</td></tr><tr><td><i>disabled</i></td><td>Disabled.</td></tr></table>	Option	Description	<i>optional</i>	Optional.	<i>mandatory</i>	Mandatory.	<i>disabled</i>	Disabled.			
Option	Description											
<i>optional</i>	Optional.											
<i>mandatory</i>	Mandatory.											
<i>disabled</i>	Disabled.											
sso-attribute-value	Name of the RADIUS user group that this local user group represents.	string	Maximum length: 511									

Parameter	Description	Type	Size	Default
user-id	Guest user ID type.	option	-	email
	<b>Option</b>	<b>Description</b>		
	<i>email</i>	Email address.		
	<i>auto-generate</i>	Automatically generate.		
	<i>specify</i>	Specify.		
user-name	Enable/disable the guest user name entry.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Enable setting.		
	<i>enable</i>	Disable setting.		

\*\* Values may differ between models.

## config guest

Parameter	Description	Type	Size	Default
id	Guest ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
user-id	Guest ID.	string	Maximum length: 64	
name	Guest name.	string	Maximum length: 64	
password	Guest password.	password	Not Specified	
mobile-phone	Mobile phone.	string	Maximum length: 35	
sponsor	Set the action for the sponsor guest user field.	string	Maximum length: 35	
company	Set the action for the company guest user field.	string	Maximum length: 35	
email	Email.	string	Maximum length: 64	
expiration	Expire time.	user	Not Specified	
comment	Comment.	var-string	Maximum length: 255	



## config match

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
server-name	Name of remote auth server.	string	Maximum length: 35	
group-name	Name of matching user or group on remote authentication server.	string	Maximum length: 511	

## config user krb-keytab

Configure Kerberos keytab entries.

```
config user krb-keytab
  Description: Configure Kerberos keytab entries.
  edit <name>
    set keytab {string}
    set ldap-server <name1>, <name2>, ...
    set pac-data [enable|disable]
    set principal {string}
  next
end
```

## config user krb-keytab

Parameter	Description	Type	Size	Default
keytab	Base64 coded keytab file containing a pre-shared key.	string	Maximum length: 8191	
ldap-server <name>	LDAP server name(s). LDAP server name.	string	Maximum length: 79	
name	Kerberos keytab entry name.	string	Maximum length: 35	
pac-data	Enable/disable parsing PAC data in the ticket.	option	-	enable
		Option	Description	
		<i>enable</i>	Enable parsing PAC data in the ticket.	
		<i>disable</i>	Disable parsing PAC data in the ticket.	
principal	Kerberos service principal. For example, HTTP/myfgt.example.com@example.com.	string	Maximum length: 511	

## config user ldap

Configure LDAP server entries.

```
config user ldap
  Description: Configure LDAP server entries.
  edit <name>
    set account-key-filter {string}
    set account-key-processing [same|strip]
    set antiphish [enable|disable]
    set ca-cert {string}
    set cnid {string}
    set dn {string}
    set group-filter {string}
    set group-member-check [user-attr|group-object|...]
    set group-object-filter {string}
    set group-search-base {string}
    set interface {string}
    set interface-select-method [auto|sdwan|...]
    set member-attr {string}
    set obtain-user-info [enable|disable]
    set password {password}
    set password-attr {string}
    set password-expiry-warning [enable|disable]
    set password-renewal [enable|disable]
    set port {integer}
    set search-type {option1}, {option2}, ...
    set secondary-server {string}
    set secure [disable|starttls|...]
    set server {string}
    set server-identity-check [enable|disable]
    set source-ip {string}
    set source-port {integer}
    set ssl-min-protocol-version [default|SSLv3|...]
    set tertiary-server {string}
    set two-factor [disable|fortitoken-cloud]
    set two-factor-authentication [fortitoken|email|...]
    set two-factor-notification [email|sms]
    set type [simple|anonymous|...]
    set user-info-exchange-server {string}
    set username {string}
  next
end
```

## config user ldap

Parameter	Description	Type	Size	Default
account-key-filter	Account key filter, using the UPN as the search filter.	string	Maximum length: 2047	(&(userPrincipalName=%s)(!(UserAccountControl:1.2.840.113556.1.4.803:=2)))

Parameter	Description	Type	Size	Default						
account-key-processing	Account key processing operation, either keep or strip domain string of UPN in the token.	option	-	same						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>same</td><td>Same as UPN.</td></tr><tr><td>strip</td><td>Strip domain string from UPN.</td></tr></table>	Option	Description	same	Same as UPN.	strip	Strip domain string from UPN.			
Option	Description									
same	Same as UPN.									
strip	Strip domain string from UPN.									
antiphish	Enable/disable AntiPhishing credential backend.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable AntiPhishing credential backend.</td></tr><tr><td>disable</td><td>Disable AntiPhishing credential backend.</td></tr></table>	Option	Description	enable	Enable AntiPhishing credential backend.	disable	Disable AntiPhishing credential backend.			
Option	Description									
enable	Enable AntiPhishing credential backend.									
disable	Disable AntiPhishing credential backend.									
ca-cert	CA certificate name.	string	Maximum length: 79							
cnid	Common name identifier for the LDAP server. The common name identifier for most LDAP servers is "cn".	string	Maximum length: 20	cn						
dn	Distinguished name used to look up entries on the LDAP server.	string	Maximum length: 511							
group-filter	Filter used for group matching.	string	Maximum length: 2047							
group-member-check	Group member checking methods.	option	-	user-attr						

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>user-attr</i>	User attribute checking.		
	<i>group-object</i>	Group object checking.		
	<i>posix-group-object</i>	POSIX group object checking.		
group-object-filter	Filter used for group searching.	string	Maximum length: 2047	(&(objectcategory=group)(member=*))
group-search-base	Search base used for group searching.	string	Maximum length: 511	
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto
	<b>Option</b>	<b>Description</b>		
	<i>auto</i>	Set outgoing interface automatically.		
	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.		
	<i>specify</i>	Set outgoing interface manually.		
member-attr	Name of attribute from which to get group membership.	string	Maximum length: 63	memberOf
name	LDAP server entry name.	string	Maximum length: 35	
obtain-user-info	Enable/disable obtaining of user information.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable obtaining of user information.		
	<i>disable</i>	Disable obtaining of user information.		

Parameter	Description	Type	Size	Default						
password	Password for initial binding.	password	Not Specified							
password-attr	Name of attribute to get password hash.	string	Maximum length: 35	userPassword						
password-expiry-warning	Enable/disable password expiry warnings.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable password expiry warnings.</td></tr><tr><td><i>disable</i></td><td>Disable password expiry warnings.</td></tr></table>				Option	Description	<i>enable</i>	Enable password expiry warnings.	<i>disable</i>	Disable password expiry warnings.
Option	Description									
<i>enable</i>	Enable password expiry warnings.									
<i>disable</i>	Disable password expiry warnings.									
password-renewal	Enable/disable online password renewal.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable online password renewal.</td></tr><tr><td><i>disable</i></td><td>Disable online password renewal.</td></tr></table>				Option	Description	<i>enable</i>	Enable online password renewal.	<i>disable</i>	Disable online password renewal.
Option	Description									
<i>enable</i>	Enable online password renewal.									
<i>disable</i>	Disable online password renewal.									
port	Port to be used for communication with the LDAP server.	integer	Minimum value: 1 Maximum value: 65535	389						
search-type	Search type.	option	-							
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>recursive</i></td><td>Recursively retrieve the user-group chain information of a user in a particular Microsoft AD domain.</td></tr></table>				Option	Description	<i>recursive</i>	Recursively retrieve the user-group chain information of a user in a particular Microsoft AD domain.		
Option	Description									
<i>recursive</i>	Recursively retrieve the user-group chain information of a user in a particular Microsoft AD domain.									
secondary-server	Secondary LDAP server CN domain name or IP.	string	Maximum length: 63							
secure	Port to be used for authentication.	option	-	disable						

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	No SSL.		
	<i>starttls</i>	Use StartTLS.		
	<i>ldaps</i>	Use LDAPS.		
server	LDAP server CN domain name or IP.	string	Maximum length: 63	
server-identity-check	Enable/disable LDAP server identity check (verify server domain name/IP address against the server certificate).	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable server identity check.		
	<i>disable</i>	Disable server identity check.		
source-ip	FortiGate IP address to be used for communication with the LDAP server.	string	Maximum length: 63	
source-port	Source port to be used for communication with the LDAP server.	integer	Minimum value: 0 Maximum value: 65535	0
ssl-min-protocol-version	Minimum supported protocol version for SSL/TLS connections.	option	-	default
	<b>Option</b>	<b>Description</b>		
	<i>default</i>	Follow system global setting.		

Parameter	Description	Type	Size	Default
	Option	Description		
	SSLv3	SSLv3.		
	TLSv1	TLSv1.		
	TLSv1-1	TLSv1.1.		
	TLSv1-2	TLSv1.2.		
tertiary-server	Tertiary LDAP server CN domain name or IP.	string	Maximum length: 63	
two-factor	Enable/disable two-factor authentication.	option	-	disable
	Option	Description		
	disable	disable two-factor authentication.		
	fortitoken-cloud	FortiToken Cloud Service.		
two-factor-authentication	Authentication method by FortiToken Cloud.	option	-	
	Option	Description		
	fortitoken	FortiToken authentication.		
	email	Email one time password.		
	sms	SMS one time password.		
two-factor-notification	Notification method for user activation by FortiToken Cloud.	option	-	
	Option	Description		
	email	Email notification for activation code.		
	sms	SMS notification for activation code.		

Parameter	Description	Type	Size	Default
type	Authentication type for LDAP searches.	option	-	simple
	<b>Option</b>	<b>Description</b>		
	<i>simple</i>	Simple password authentication without search.		
	<i>anonymous</i>	Bind using anonymous user search.		
	<i>regular</i>	Bind using username/password and then search.		
user-info-exchange-server	MS Exchange server from which to fetch user information.	string	Maximum length: 35	
username	Username (full DN) for initial binding.	string	Maximum length: 511	

## config user local

Configure local users.

```
config user local
  Description: Configure local users.
  edit <name>
    set auth-concurrent-override [enable|disable]
    set auth-concurrent-value {integer}
    set authtimeout {integer}
    set email-to {string}
    set fortitoken {string}
    set id {integer}
    set ldap-server {string}
    set passwd {password}
    set passwd-policy {string}
    set passwd-time {user}
    set ppk-identity {string}
    set ppk-secret {password-3}
    set radius-server {string}
    set sms-custom-server {string}
    set sms-phone {string}
    set sms-server [fortiguard|custom]
    set status [enable|disable]
    set tacacs+-server {string}
    set two-factor [disable|fortitoken|...]
    set two-factor-authentication [fortitoken|email|...]
    set two-factor-notification [email|sms]
    set type [password|radius|...]
    set username-sensitivity [disable|enable]
    set workstation {string}
```



next  
end

## config user local

Parameter	Description	Type	Size	Default
auth-concurrent-override	Enable/disable overriding the policy-auth-concurrent under config system global.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable auth-concurrent-override.		
	<i>disable</i>	Disable auth-concurrent-override.		
auth-concurrent-value	Maximum number of concurrent logins permitted from the same user.	integer	Minimum value: 0 Maximum value: 100	0
authtimeout	Time in minutes before the authentication timeout for a user is reached.	integer	Minimum value: 0 Maximum value: 1440	0
email-to	Two-factor recipient's email address.	string	Maximum length: 63	
fortitoken	Two-factor recipient's FortiToken serial number.	string	Maximum length: 16	
id	User ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
ldap-server	Name of LDAP server with which the user must authenticate.	string	Maximum length: 35	
name	User name.	string	Maximum length: 64	
passwd	User's password.	password	Not Specified	
passwd-policy	Password policy to apply to this user, as defined in config user password-policy.	string	Maximum length: 35	
passwd-time	Time of the last password update.	user	Not Specified	
ppk-identity	IKEv2 Postquantum Preshared Key Identity.	string	Maximum length: 35	

Parameter	Description	Type	Size	Default												
ppk-secret	IKEv2 Postquantum Preshared Key (ASCII string or hexadecimal encoded with a leading 0x).	password-3	Not Specified													
radius-server	Name of RADIUS server with which the user must authenticate.	string	Maximum length: 35													
sms-custom-server	Two-factor recipient's SMS server.	string	Maximum length: 35													
sms-phone	Two-factor recipient's mobile phone number.	string	Maximum length: 15													
sms-server	Send SMS through FortiGuard or other external server.	option	-	fortiguard												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>fortiguard</i></td><td>Send SMS by FortiGuard.</td></tr><tr><td><i>custom</i></td><td>Send SMS by custom server.</td></tr></table>				Option	Description	<i>fortiguard</i>	Send SMS by FortiGuard.	<i>custom</i>	Send SMS by custom server.						
	Option	Description														
	<i>fortiguard</i>	Send SMS by FortiGuard.														
<i>custom</i>	Send SMS by custom server.															
status	Enable/disable allowing the local user to authenticate with the FortiGate unit.	option	-	enable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable user.</td></tr><tr><td><i>disable</i></td><td>Disable user.</td></tr></table>				Option	Description	<i>enable</i>	Enable user.	<i>disable</i>	Disable user.						
	Option	Description														
	<i>enable</i>	Enable user.														
<i>disable</i>	Disable user.															
tacacs+-server	Name of TACACS+ server with which the user must authenticate.	string	Maximum length: 35													
two-factor	Enable/disable two-factor authentication.	option	-	disable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>disable</td></tr><tr><td><i>fortitoken</i></td><td>FortiToken</td></tr><tr><td><i>fortitoken-cloud</i></td><td>FortiToken Cloud Service.</td></tr><tr><td><i>email</i></td><td>Email authentication code.</td></tr><tr><td><i>sms</i></td><td>SMS authentication code.</td></tr></table>				Option	Description	<i>disable</i>	disable	<i>fortitoken</i>	FortiToken	<i>fortitoken-cloud</i>	FortiToken Cloud Service.	<i>email</i>	Email authentication code.	<i>sms</i>	SMS authentication code.
	Option	Description														
	<i>disable</i>	disable														
	<i>fortitoken</i>	FortiToken														
	<i>fortitoken-cloud</i>	FortiToken Cloud Service.														
	<i>email</i>	Email authentication code.														
<i>sms</i>	SMS authentication code.															
two-factor-authentication	Authentication method by FortiToken Cloud.	option	-													
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>fortitoken</i></td><td>FortiToken authentication.</td></tr></table>				Option	Description	<i>fortitoken</i>	FortiToken authentication.								
	Option	Description														
<i>fortitoken</i>	FortiToken authentication.															

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>email</i>	Email one time password.		
	<i>sms</i>	SMS one time password.		
two-factor-notification	Notification method for user activation by FortiToken Cloud.	option	-	
	<b>Option</b>	<b>Description</b>		
	<i>email</i>	Email notification for activation code.		
	<i>sms</i>	SMS notification for activation code.		
type	Authentication method.	option	-	password
	<b>Option</b>	<b>Description</b>		
	<i>password</i>	Password authentication.		
	<i>radius</i>	RADIUS server authentication.		
	<i>tacacs+</i>	TACACS+ server authentication.		
	<i>ldap</i>	LDAP server authentication.		
username-sensitivity	Enable/disable case and accent sensitivity when performing username matching (accents are stripped and case is ignored when disabled).	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Ignore case and accents. Username at prompt not required to match case or accents.		
	<i>enable</i>	Do not ignore case and accents. Username at prompt must be an exact match.		
workstation	Name of the remote user workstation, if you want to limit the user to authenticate only from a particular workstation.	string	Maximum length: 35	

## config user nac-policy

Configure NAC policy matching pattern to identify matching NAC devices.

```
config user nac-policy
  Description: Configure NAC policy matching pattern to identify matching NAC devices.
  edit <name>
    set category [device|firewall-user|...]
    set description {string}
    set ems-tag {string}
```

```

set family {string}
set firewall-address {string}
set host {string}
set hw-vendor {string}
set hw-version {string}
set mac {string}
set os {string}
set src {string}
set ssid-policy {string}
set status [enable|disable]
set sw-version {string}
set switch-fortilink {string}
set switch-group <name1>, <name2>, ...
set switch-mac-policy {string}
set type {string}
set user {string}
set user-group {string}
next
end

```

## config user nac-policy

Parameter	Description	Type	Size	Default
category	Category of NAC policy.	option	-	device
	<b>Option</b>	<b>Description</b>		
	<i>device</i>	Device category.		
	<i>firewall-user</i>	Firewall user category.		
	<i>ems-tag</i>	EMS Tag category.		
description	Description for the NAC policy matching pattern.	string	Maximum length: 63	
ems-tag	NAC policy matching EMS tag.	string	Maximum length: 79	
family	NAC policy matching family.	string	Maximum length: 31	
firewall-address *	Dynamic firewall address to associate MAC which match this policy.	string	Maximum length: 79	
host	NAC policy matching host.	string	Maximum length: 64	
hw-vendor	NAC policy matching hardware vendor.	string	Maximum length: 15	
hw-version	NAC policy matching hardware version.	string	Maximum length: 15	

Parameter	Description	Type	Size	Default						
mac	NAC policy matching MAC address.	string	Maximum length: 17							
name	NAC policy name.	string	Maximum length: 63							
os	NAC policy matching operating system.	string	Maximum length: 31							
src	NAC policy matching source.	string	Maximum length: 15							
ssid-policy	SSID policy to be applied on the matched NAC policy.	string	Maximum length: 35							
status	Enable/disable NAC policy.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable NAC policy.</td></tr><tr><td><i>disable</i></td><td>Disable NAC policy.</td></tr></table>				Option	Description	<i>enable</i>	Enable NAC policy.	<i>disable</i>	Disable NAC policy.
Option	Description									
<i>enable</i>	Enable NAC policy.									
<i>disable</i>	Disable NAC policy.									
sw-version	NAC policy matching software version.	string	Maximum length: 15							
switch-fortilink *	FortiLink interface for which this NAC policy belongs to.	string	Maximum length: 15							
switch-group <name> *	List of managed FortiSwitch groups on which NAC policy can be applied. Managed FortiSwitch group name from available options.	string	Maximum length: 79							
switch-mac-policy *	Switch MAC policy action to be applied on the matched NAC policy.	string	Maximum length: 63							
type	NAC policy matching type.	string	Maximum length: 15							
user	NAC policy matching user.	string	Maximum length: 64							
user-group	NAC policy matching user group.	string	Maximum length: 35							

\* This parameter may not exist in some models.

## config user password-policy

Configure user password policy.

```
config user password-policy
    Description: Configure user password policy.
```

```

edit <name>
    set expire-days {integer}
    set expired-password-renewal [enable|disable]
    set warn-days {integer}
next
end

```

## config user password-policy

Parameter	Description	Type	Size	Default						
expire-days	Time in days before the user's password expires.	integer	Minimum value: 0 Maximum value: 999	180						
expired-password-renewal	Enable/disable renewal of a password that already is expired.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable renewal of a password that already is expired.</td></tr><tr><td><i>disable</i></td><td>Disable renewal of a password that already is expired.</td></tr></table>				Option	Description	<i>enable</i>	Enable renewal of a password that already is expired.	<i>disable</i>	Disable renewal of a password that already is expired.
Option	Description									
<i>enable</i>	Enable renewal of a password that already is expired.									
<i>disable</i>	Disable renewal of a password that already is expired.									
name	Password policy name.	string	Maximum length: 35							
warn-days	Time in days before a password expiration warning message is displayed to the user upon login.	integer	Minimum value: 0 Maximum value: 30	15						

## config user peer

Configure peer users.

```

config user peer
    Description: Configure peer users.
    edit <name>
        set ca {string}
        set cn {string}
        set cn-type [string|email|...]
        set ldap-mode [password|principal-name]
        set ldap-password {password}
        set ldap-server {string}
        set ldap-username {string}
        set mandatory-ca-verify [enable|disable]
        set ocsf-override-server {string}
        set passwd {password}
        set subject {string}
        set two-factor [enable|disable]
    end
end

```

next  
end

## config user peer

Parameter	Description	Type	Size	Default												
ca	Name of the CA certificate.	string	Maximum length: 127													
cn	Peer certificate common name.	string	Maximum length: 255													
cn-type	Peer certificate common name type.	option	-	string												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>string</i></td><td>Normal string.</td></tr><tr><td><i>email</i></td><td>Email address.</td></tr><tr><td><i>FQDN</i></td><td>Fully Qualified Domain Name.</td></tr><tr><td><i>ipv4</i></td><td>IPv4 address.</td></tr><tr><td><i>ipv6</i></td><td>IPv6 address.</td></tr></table>	Option	Description	<i>string</i>	Normal string.	<i>email</i>	Email address.	<i>FQDN</i>	Fully Qualified Domain Name.	<i>ipv4</i>	IPv4 address.	<i>ipv6</i>	IPv6 address.			
	Option	Description														
	<i>string</i>	Normal string.														
	<i>email</i>	Email address.														
	<i>FQDN</i>	Fully Qualified Domain Name.														
	<i>ipv4</i>	IPv4 address.														
<i>ipv6</i>	IPv6 address.															
ldap-mode	Mode for LDAP peer authentication.	option	-	password												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>password</i></td><td>Username/password.</td></tr><tr><td><i>principal-name</i></td><td>Principal name.</td></tr></table>	Option	Description	<i>password</i>	Username/password.	<i>principal-name</i>	Principal name.									
	Option	Description														
	<i>password</i>	Username/password.														
<i>principal-name</i>	Principal name.															
ldap-password	Password for LDAP server bind.	password	Not Specified													
ldap-server	Name of an LDAP server defined under the user ldap command. Performs client access rights check.	string	Maximum length: 35													
ldap-username	Username for LDAP server bind.	string	Maximum length: 35													
mandatory-ca-verify	Determine what happens to the peer if the CA certificate is not installed. Disable to automatically consider the peer certificate as valid.	option	-	enable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.									
	Option	Description														
	<i>enable</i>	Enable setting.														
<i>disable</i>	Disable setting.															
name	Peer name.	string	Maximum length: 35													

Parameter	Description	Type	Size	Default						
ocsp-override-server	Online Certificate Status Protocol (OCSP) server for certificate retrieval.	string	Maximum length: 35							
passwd	Peer's password used for two-factor authentication.	password	Not Specified							
subject	Peer certificate name constraints.	string	Maximum length: 255							
two-factor	Enable/disable two-factor authentication, applying certificate and password-based authentication.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable 2-factor authentication.</td></tr><tr><td><i>disable</i></td><td>Disable 2-factor authentication.</td></tr></table>				Option	Description	<i>enable</i>	Enable 2-factor authentication.	<i>disable</i>	Disable 2-factor authentication.
Option	Description									
<i>enable</i>	Enable 2-factor authentication.									
<i>disable</i>	Disable 2-factor authentication.									

## config user peergrp

Configure peer groups.

```
config user peergrp
    Description: Configure peer groups.
    edit <name>
        set member <name1>, <name2>, ...
    next
end
```

## config user peergrp

Parameter	Description	Type	Size	Default
member <name>	Peer group members. Peer group member name.	string	Maximum length: 35	
name	Peer group name.	string	Maximum length: 35	

## config user pop3

POP3 server entry configuration.

```
config user pop3
    Description: POP3 server entry configuration.
    edit <name>
        set port {integer}
        set secure [none|starttls|...]
    next
end
```



```

        set server {string}
        set ssl-min-proto-version [default|SSLv3|...]
    next
end

```

## config user pop3

Parameter	Description	Type	Size	Default												
name	POP3 server entry name.	string	Maximum length: 35													
port	POP3 service port number.	integer	Minimum value: 0 Maximum value: 65535	0												
secure	SSL connection.	option	-	starttls												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>None.</td></tr><tr><td><i>starttls</i></td><td>Use StartTLS.</td></tr><tr><td><i>pop3s</i></td><td>Use POP3 over SSL.</td></tr></table>				Option	Description	<i>none</i>	None.	<i>starttls</i>	Use StartTLS.	<i>pop3s</i>	Use POP3 over SSL.				
Option	Description															
<i>none</i>	None.															
<i>starttls</i>	Use StartTLS.															
<i>pop3s</i>	Use POP3 over SSL.															
server	Server domain name or IP address.	string	Maximum length: 63													
ssl-min-protocol-version	Minimum supported protocol version for SSL/TLS connections.	option	-	default												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>Follow system global setting.</td></tr><tr><td><i>SSLv3</i></td><td>SSLv3.</td></tr><tr><td><i>TLSv1</i></td><td>TLSv1.</td></tr><tr><td><i>TLSv1-1</i></td><td>TLSv1.1.</td></tr><tr><td><i>TLSv1-2</i></td><td>TLSv1.2.</td></tr></table>				Option	Description	<i>default</i>	Follow system global setting.	<i>SSLv3</i>	SSLv3.	<i>TLSv1</i>	TLSv1.	<i>TLSv1-1</i>	TLSv1.1.	<i>TLSv1-2</i>	TLSv1.2.
Option	Description															
<i>default</i>	Follow system global setting.															
<i>SSLv3</i>	SSLv3.															
<i>TLSv1</i>	TLSv1.															
<i>TLSv1-1</i>	TLSv1.1.															
<i>TLSv1-2</i>	TLSv1.2.															

## config user quarantine

Configure quarantine support.

```

config user quarantine
    Description: Configure quarantine support.
    set firewall-groups {string}
    set quarantine [enable|disable]
    config targets

```

```

Description: Quarantine entry to hold multiple MACs.
edit <entry>
    set description {string}
    config macs
        Description: Quarantine MACs.
        edit <mac>
            set description {string}
            set drop [disable|enable]
            set parent {string}
        next
    end
end
next
end
set traffic-policy {string}
end

```

## config user quarantine

Parameter	Description	Type	Size	Default
firewall-groups	Firewall address group which includes all quarantine MAC address.	string	Maximum length: 79	
quarantine	Enable/disable quarantine.	option	-	enable
	Option	Description		
	enable	Enable quarantine.		
	disable	Disable quarantine.		
traffic-policy *	Traffic policy for quarantined MACs.	string	Maximum length: 63	

\* This parameter may not exist in some models.

## config targets

Parameter	Description	Type	Size	Default
entry	Quarantine entry name.	string	Maximum length: 63	
description	Description for the quarantine entry.	string	Maximum length: 63	

## config macs

Parameter	Description	Type	Size	Default
mac	Quarantine MAC.	mac-address	Not Specified	00:00:00:00:00:00

Parameter	Description	Type	Size	Default						
description	Description for the quarantine MAC.	string	Maximum length: 63							
drop	Enable/disable dropping of quarantined device traffic.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Sends quarantined device traffic to FortiGate.</td></tr><tr><td><i>enable</i></td><td>Blocks quarantined device traffic to FortiGate.</td></tr></table>				Option	Description	<i>disable</i>	Sends quarantined device traffic to FortiGate.	<i>enable</i>	Blocks quarantined device traffic to FortiGate.
	Option	Description								
	<i>disable</i>	Sends quarantined device traffic to FortiGate.								
<i>enable</i>	Blocks quarantined device traffic to FortiGate.									
parent	Parent entry name.	string	Maximum length: 63							

## config user radius

Configure RADIUS server entries.

```

config user radius
    Description: Configure RADIUS server entries.
    edit <name>
        config accounting-server
            Description: Additional accounting servers.
            edit <id>
                set status [enable|disable]
                set server {string}
                set secret {password}
                set port {integer}
                set source-ip {string}
                set interface-select-method [auto|sdwan|...]
                set interface {string}
            next
        end
        set acct-all-servers [enable|disable]
        set acct-interim-interval {integer}
        set all-usergroup [disable|enable]
        set auth-type [auto|ms_chap_v2|...]
        set class <name1>, <name2>, ...
        set group-override-attr-type [filter-Id|class]
        set h3c-compatibility [enable|disable]
        set interface {string}
        set interface-select-method [auto|sdwan|...]
        set nas-ip {ipv4-address}
        set password-encoding [auto|ISO-8859-1]
        set password-renewal [enable|disable]
        set radius-coa [enable|disable]
        set radius-port {integer}
        set rsoo [enable|disable]
        set rsoo-context-timeout {integer}
        set rsoo-endpoint-attribute [User-Name|NAS-IP-Address|...]
        set rsoo-endpoint-block-attribute [User-Name|NAS-IP-Address|...]
        set rsoo-ep-one-ip-only [enable|disable]
    
```

```

set rso-flush-ip-session [enable|disable]
set rso-log-flags {option1}, {option2}, ...
set rso-log-period {integer}
set rso-radius-response [enable|disable]
set rso-radius-server-port {integer}
set rso-secret {password}
set rso-validate-request-secret [enable|disable]
set secondary-secret {password}
set secondary-server {string}
set secret {password}
set server {string}
set source-ip {string}
set sso-attribute [User-Name|NAS-IP-Address|...]
set sso-attribute-key {string}
set sso-attribute-value-override [enable|disable]
set switch-controller-acct-fast-framedip-detect {integer}
set switch-controller-service-type {option1}, {option2}, ...
set tertiary-secret {password}
set tertiary-server {string}
set timeout {integer}
set use-management-vdom [enable|disable]
set username-case-sensitive [enable|disable]
next
end

```

## config user radius

Parameter	Description	Type	Size	Default						
acct-all-servers	Enable/disable sending of accounting messages to all configured servers.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Send accounting messages to all configured servers.</td></tr><tr><td><i>disable</i></td><td>Send accounting message only to servers that are confirmed to be reachable.</td></tr></table>	Option	Description	<i>enable</i>	Send accounting messages to all configured servers.	<i>disable</i>	Send accounting message only to servers that are confirmed to be reachable.			
Option	Description									
<i>enable</i>	Send accounting messages to all configured servers.									
<i>disable</i>	Send accounting message only to servers that are confirmed to be reachable.									
acct-interim-interval	Time in seconds between each accounting interim update message.	integer	Minimum value: 60 Maximum value: 86400	0						
all-usergroup	Enable/disable automatically including this RADIUS server in all user groups.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Do not automatically include this server in a user group.</td></tr><tr><td><i>enable</i></td><td>Include this RADIUS server in every user group.</td></tr></table>	Option	Description	<i>disable</i>	Do not automatically include this server in a user group.	<i>enable</i>	Include this RADIUS server in every user group.			
Option	Description									
<i>disable</i>	Do not automatically include this server in a user group.									
<i>enable</i>	Include this RADIUS server in every user group.									

Parameter	Description	Type	Size	Default												
auth-type	Authentication methods/protocols permitted for this RADIUS server.	option	-	auto												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>auto</td><td>Use PAP, MSCHAP_v2, and CHAP (in that order).</td></tr><tr><td>ms_chap_v2</td><td>Microsoft Challenge Handshake Authentication Protocol version 2.</td></tr><tr><td>ms_chap</td><td>Microsoft Challenge Handshake Authentication Protocol.</td></tr><tr><td>chap</td><td>Challenge Handshake Authentication Protocol.</td></tr><tr><td>pap</td><td>Password Authentication Protocol.</td></tr></table>	Option	Description	auto	Use PAP, MSCHAP_v2, and CHAP (in that order).	ms_chap_v2	Microsoft Challenge Handshake Authentication Protocol version 2.	ms_chap	Microsoft Challenge Handshake Authentication Protocol.	chap	Challenge Handshake Authentication Protocol.	pap	Password Authentication Protocol.			
Option	Description															
auto	Use PAP, MSCHAP_v2, and CHAP (in that order).															
ms_chap_v2	Microsoft Challenge Handshake Authentication Protocol version 2.															
ms_chap	Microsoft Challenge Handshake Authentication Protocol.															
chap	Challenge Handshake Authentication Protocol.															
pap	Password Authentication Protocol.															
class <name>	Class attribute name(s). Class name.	string	Maximum length: 79													
group-override-attr-type	RADIUS attribute type to override user group information.	option	-													
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>filter-ld</td><td>Filter-Id</td></tr><tr><td>class</td><td>Class</td></tr></table>	Option	Description	filter-ld	Filter-Id	class	Class									
Option	Description															
filter-ld	Filter-Id															
class	Class															
h3c-compatibility	Enable/disable compatibility with the H3C, a mechanism that performs security checking for authentication.	option	-	disable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable H3C compatibility.</td></tr><tr><td>disable</td><td>Disable H3C compatibility.</td></tr></table>	Option	Description	enable	Enable H3C compatibility.	disable	Disable H3C compatibility.									
Option	Description															
enable	Enable H3C compatibility.															
disable	Disable H3C compatibility.															
interface	Specify outgoing interface to reach server.	string	Maximum length: 15													
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>auto</td><td>Set outgoing interface automatically.</td></tr><tr><td>sdwan</td><td>Set outgoing interface by SD-WAN or policy routing rules.</td></tr><tr><td>specify</td><td>Set outgoing interface manually.</td></tr></table>	Option	Description	auto	Set outgoing interface automatically.	sdwan	Set outgoing interface by SD-WAN or policy routing rules.	specify	Set outgoing interface manually.							
Option	Description															
auto	Set outgoing interface automatically.															
sdwan	Set outgoing interface by SD-WAN or policy routing rules.															
specify	Set outgoing interface manually.															
name	RADIUS server entry name.	string	Maximum length: 35													

Parameter	Description	Type	Size	Default
nas-ip	IP address used to communicate with the RADIUS server and used as NAS-IP-Address and Called-Station-ID attributes.	ipv4-address	Not Specified	0.0.0.0
password-encoding	Password encoding.	option	-	auto
	Option	Description		
	auto	Use original password encoding.		
	ISO-8859-1	Use ISO-8859-1 password encoding.		
password-renewal	Enable/disable password renewal.	option	-	enable
	Option	Description		
	enable	Enable password renewal.		
	disable	Disable password renewal.		
radius-coa	Enable to allow a mechanism to change the attributes of an authentication, authorization, and accounting session after it is authenticated.	option	-	disable
	Option	Description		
	enable	Enable RADIUS CoA.		
	disable	Disable RADIUS CoA.		
radius-port	RADIUS service port number.	integer	Minimum value: 0 Maximum value: 65535	0
rsso	Enable/disable RADIUS based single sign on feature.	option	-	disable
	Option	Description		
	enable	Enable RADIUS based single sign on feature.		
	disable	Disable RADIUS based single sign on feature.		
rsso-context-timeout	Time in seconds before the logged out user is removed from the "user context list" of logged on users.	integer	Minimum value: 0 Maximum value: 4294967295	28800

Parameter	Description	Type	Size	Default
rsso-endpoint-attribute	RADIUS attributes used to extract the user end point identifier from the RADIUS Start record.	option	-	Calling-Station-Id
	<b>Option</b>	<b>Description</b>		
	User-Name	Use this attribute.		
	NAS-IP-Address	Use this attribute.		
	Framed-IP-Address	Use this attribute.		
	Framed-IP-Netmask	Use this attribute.		
	Filter-Id	Use this attribute.		
	Login-IP-Host	Use this attribute.		
	Reply-Message	Use this attribute.		
	Callback-Number	Use this attribute.		
	Callback-Id	Use this attribute.		
	Framed-Route	Use this attribute.		
	Framed-IPX-Network	Use this attribute.		
	Class	Use this attribute.		
	Called-Station-Id	Use this attribute.		
	Calling-Station-Id	Use this attribute.		
	NAS-Identifier	Use this attribute.		
	Proxy-State	Use this attribute.		
	Login-LAT-Service	Use this attribute.		
	Login-LAT-Node	Use this attribute.		
	Login-LAT-Group	Use this attribute.		
Framed-AppleTalk-Zone	Use this attribute.			
Acct-Session-Id	Use this attribute.			
Acct-Multi-Session-Id	Use this attribute.			

Parameter	Description	Type	Size	Default
rsso-endpoint-block-attribute	RADIUS attributes used to block a user.	option	-	
	<b>Option</b>	<b>Description</b>		
	User-Name	Use this attribute.		
	NAS-IP-Address	Use this attribute.		
	Framed-IP-Address	Use this attribute.		
	Framed-IP-Netmask	Use this attribute.		
	Filter-Id	Use this attribute.		
	Login-IP-Host	Use this attribute.		
	Reply-Message	Use this attribute.		
	Callback-Number	Use this attribute.		
	Callback-Id	Use this attribute.		
	Framed-Route	Use this attribute.		
	Framed-IPX-Network	Use this attribute.		
	Class	Use this attribute.		
	Called-Station-Id	Use this attribute.		
	Calling-Station-Id	Use this attribute.		
	NAS-Identifier	Use this attribute.		
	Proxy-State	Use this attribute.		
	Login-LAT-Service	Use this attribute.		
	Login-LAT-Node	Use this attribute.		
	Login-LAT-Group	Use this attribute.		
Framed-AppleTalk-Zone	Use this attribute.			
Acct-Session-Id	Use this attribute.			
Acct-Multi-Session-Id	Use this attribute.			



Parameter	Description	Type	Size	Default																
rsso-ep-one-ip-only	Enable/disable the replacement of old IP addresses with new ones for the same endpoint on RADIUS accounting Start messages.	option	-	disable																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable replacement of old IP address with new IP address for the same endpoint on RADIUS accounting start.</td></tr><tr><td><i>disable</i></td><td>Disable replacement of old IP address with new IP address for the same endpoint on RADIUS accounting start.</td></tr></table>	Option	Description	<i>enable</i>	Enable replacement of old IP address with new IP address for the same endpoint on RADIUS accounting start.	<i>disable</i>	Disable replacement of old IP address with new IP address for the same endpoint on RADIUS accounting start.													
Option	Description																			
<i>enable</i>	Enable replacement of old IP address with new IP address for the same endpoint on RADIUS accounting start.																			
<i>disable</i>	Disable replacement of old IP address with new IP address for the same endpoint on RADIUS accounting start.																			
rsso-flush-ip-session	Enable/disable flushing user IP sessions on RADIUS accounting Stop messages.	option	-	disable																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable flush user IP sessions on RADIUS accounting stop.</td></tr><tr><td><i>disable</i></td><td>Disable flush user IP sessions on RADIUS accounting stop.</td></tr></table>	Option	Description	<i>enable</i>	Enable flush user IP sessions on RADIUS accounting stop.	<i>disable</i>	Disable flush user IP sessions on RADIUS accounting stop.													
Option	Description																			
<i>enable</i>	Enable flush user IP sessions on RADIUS accounting stop.																			
<i>disable</i>	Disable flush user IP sessions on RADIUS accounting stop.																			
rsso-log-flags	Events to log.	option	-	protocol-error profile-missing accounting-stop-missed accounting-event endpoint-block radiusd-other																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>protocol-error</i></td><td>Enable this log type.</td></tr><tr><td><i>profile-missing</i></td><td>Enable this log type.</td></tr><tr><td><i>accounting-stop-missed</i></td><td>Enable this log type.</td></tr><tr><td><i>accounting-event</i></td><td>Enable this log type.</td></tr><tr><td><i>endpoint-block</i></td><td>Enable this log type.</td></tr><tr><td><i>radiusd-other</i></td><td>Enable this log type.</td></tr><tr><td><i>none</i></td><td>Disable all logging.</td></tr></table>	Option	Description	<i>protocol-error</i>	Enable this log type.	<i>profile-missing</i>	Enable this log type.	<i>accounting-stop-missed</i>	Enable this log type.	<i>accounting-event</i>	Enable this log type.	<i>endpoint-block</i>	Enable this log type.	<i>radiusd-other</i>	Enable this log type.	<i>none</i>	Disable all logging.			
Option	Description																			
<i>protocol-error</i>	Enable this log type.																			
<i>profile-missing</i>	Enable this log type.																			
<i>accounting-stop-missed</i>	Enable this log type.																			
<i>accounting-event</i>	Enable this log type.																			
<i>endpoint-block</i>	Enable this log type.																			
<i>radiusd-other</i>	Enable this log type.																			
<i>none</i>	Disable all logging.																			

Parameter	Description	Type	Size	Default
rsso-log-period	Time interval in seconds that group event log messages will be generated for dynamic profile events.	integer	Minimum value: 0 Maximum value: 4294967295	0
rsso-radius-response	Enable/disable sending RADIUS response packets after receiving Start and Stop records.	option	-	disable
	<b>Option</b>		<b>Description</b>	
	<i>enable</i>		Enable sending RADIUS response packets.	
	<i>disable</i>		Disable sending RADIUS response packets.	
rsso-radius-server-port	UDP port to listen on for RADIUS Start and Stop records.	integer	Minimum value: 0 Maximum value: 65535	1813
rsso-secret	RADIUS secret used by the RADIUS accounting server.	password	Not Specified	
rsso-validate-request-secret	Enable/disable validating the RADIUS request shared secret in the Start or End record.	option	-	disable
	<b>Option</b>		<b>Description</b>	
	<i>enable</i>		Enable validating RADIUS request shared secret.	
	<i>disable</i>		Disable validating RADIUS request shared secret.	
secondary-secret	Secret key to access the secondary server.	password	Not Specified	
secondary-server	Secondary RADIUS CN domain name or IP address.	string	Maximum length: 63	
secret	Pre-shared secret key used to access the primary RADIUS server.	password	Not Specified	
server	Primary RADIUS server CN domain name or IP address.	string	Maximum length: 63	
source-ip	Source IP address for communications to the RADIUS server.	string	Maximum length: 63	
sso-attribute	RADIUS attribute that contains the profile group name to be extracted from the RADIUS Start record.	option	-	Class

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>User-Name</i>	Use this attribute.		
	<i>NAS-IP-Address</i>	Use this attribute.		
	<i>Framed-IP-Address</i>	Use this attribute.		
	<i>Framed-IP-Netmask</i>	Use this attribute.		
	<i>Filter-Id</i>	Use this attribute.		
	<i>Login-IP-Host</i>	Use this attribute.		
	<i>Reply-Message</i>	Use this attribute.		
	<i>Callback-Number</i>	Use this attribute.		
	<i>Callback-Id</i>	Use this attribute.		
	<i>Framed-Route</i>	Use this attribute.		
	<i>Framed-IPX-Network</i>	Use this attribute.		
	<i>Class</i>	Use this attribute.		
	<i>Called-Station-Id</i>	Use this attribute.		
	<i>Calling-Station-Id</i>	Use this attribute.		
	<i>NAS-Identifier</i>	Use this attribute.		
	<i>Proxy-State</i>	Use this attribute.		
	<i>Login-LAT-Service</i>	Use this attribute.		
	<i>Login-LAT-Node</i>	Use this attribute.		
	<i>Login-LAT-Group</i>	Use this attribute.		
	<i>Framed-AppleTalk-Zone</i>	Use this attribute.		
	<i>Acct-Session-Id</i>	Use this attribute.		
	<i>Acct-Multi-Session-Id</i>	Use this attribute.		

Parameter	Description	Type	Size	Default																								
sso-attribute-key	Key prefix for SSO group value in the SSO attribute.	string	Maximum length: 35																									
sso-attribute-value-override	Enable/disable override old attribute value with new value for the same endpoint.	option	-	enable																								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable override old attribute value with new value for the same endpoint.</td></tr><tr><td>disable</td><td>Disable override old attribute value with new value for the same endpoint.</td></tr></table>				Option	Description	enable	Enable override old attribute value with new value for the same endpoint.	disable	Disable override old attribute value with new value for the same endpoint.																		
Option	Description																											
enable	Enable override old attribute value with new value for the same endpoint.																											
disable	Disable override old attribute value with new value for the same endpoint.																											
switch-controller-acct-fast-framedip-detect	Switch controller accounting message Framed-IP detection from DHCP snooping.	integer	Minimum value: 2 Maximum value: 600	2																								
switch-controller-service-type	RADIUS service type.	option	-																									
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>login</td><td>User should be connected to a host.</td></tr><tr><td>framed</td><td>User use Framed Protocol.</td></tr><tr><td>callback-login</td><td>User disconnected and called back.</td></tr><tr><td>callback-framed</td><td>User disconnected and called back, then a Framed Protocol.</td></tr><tr><td>outbound</td><td>User granted access to outgoing devices.</td></tr><tr><td>administrative</td><td>User granted access to the administrative unsigned interface.</td></tr><tr><td>nas-prompt</td><td>User provided a command prompt on the NAS.</td></tr><tr><td>authenticate-only</td><td>Authentication requested, and no auth info needs to be returned.</td></tr><tr><td>callback-nas-prompt</td><td>User disconnected and called back, then provided a command prompt.</td></tr><tr><td>call-check</td><td>Used by the NAS in an Access-Request packet, Access-Accept to answer the call.</td></tr><tr><td>callback-administrative</td><td>User disconnected and called back, granted access to the admin unsigned interface.</td></tr></table>				Option	Description	login	User should be connected to a host.	framed	User use Framed Protocol.	callback-login	User disconnected and called back.	callback-framed	User disconnected and called back, then a Framed Protocol.	outbound	User granted access to outgoing devices.	administrative	User granted access to the administrative unsigned interface.	nas-prompt	User provided a command prompt on the NAS.	authenticate-only	Authentication requested, and no auth info needs to be returned.	callback-nas-prompt	User disconnected and called back, then provided a command prompt.	call-check	Used by the NAS in an Access-Request packet, Access-Accept to answer the call.	callback-administrative	User disconnected and called back, granted access to the admin unsigned interface.
Option	Description																											
login	User should be connected to a host.																											
framed	User use Framed Protocol.																											
callback-login	User disconnected and called back.																											
callback-framed	User disconnected and called back, then a Framed Protocol.																											
outbound	User granted access to outgoing devices.																											
administrative	User granted access to the administrative unsigned interface.																											
nas-prompt	User provided a command prompt on the NAS.																											
authenticate-only	Authentication requested, and no auth info needs to be returned.																											
callback-nas-prompt	User disconnected and called back, then provided a command prompt.																											
call-check	Used by the NAS in an Access-Request packet, Access-Accept to answer the call.																											
callback-administrative	User disconnected and called back, granted access to the admin unsigned interface.																											
tertiary-secret	Secret key to access the tertiary server.	password	Not Specified																									
tertiary-server	Tertiary RADIUS CN domain name or IP address.	string	Maximum length: 63																									

Parameter	Description	Type	Size	Default						
timeout	Time in seconds between re-sending authentication requests.	integer	Minimum value: 1 Maximum value: 300	5						
use-management-vdom	Enable/disable using management VDOM to send requests.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Send requests using the management VDOM.</td></tr><tr><td><i>disable</i></td><td>Send requests using the current VDOM.</td></tr></table>				Option	Description	<i>enable</i>	Send requests using the management VDOM.	<i>disable</i>	Send requests using the current VDOM.
Option	Description									
<i>enable</i>	Send requests using the management VDOM.									
<i>disable</i>	Send requests using the current VDOM.									
username-case-sensitive	Enable/disable case sensitive user names.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable username case-sensitive.</td></tr><tr><td><i>disable</i></td><td>Disable username case-sensitive.</td></tr></table>				Option	Description	<i>enable</i>	Enable username case-sensitive.	<i>disable</i>	Disable username case-sensitive.
Option	Description									
<i>enable</i>	Enable username case-sensitive.									
<i>disable</i>	Disable username case-sensitive.									

## config accounting-server

Parameter	Description	Type	Size	Default						
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0						
status	Status.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Log to remote syslog server.</td></tr><tr><td><i>disable</i></td><td>Do not log to remote syslog server.</td></tr></table>				Option	Description	<i>enable</i>	Log to remote syslog server.	<i>disable</i>	Do not log to remote syslog server.
	Option	Description								
	<i>enable</i>	Log to remote syslog server.								
<i>disable</i>	Do not log to remote syslog server.									
server	Server CN domain name or IP address.	string	Maximum length: 63							
secret	Secret key.	password	Not Specified							
port	RADIUS accounting port number.	integer	Minimum value: 0 Maximum value: 65535	0						

Parameter	Description	Type	Size	Default								
source-ip	Source IP address for communications to the RADIUS server.	string	Maximum length: 63									
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto</i></td><td>Set outgoing interface automatically.</td></tr><tr><td><i>sdwan</i></td><td>Set outgoing interface by SD-WAN or policy routing rules.</td></tr><tr><td><i>specify</i></td><td>Set outgoing interface manually.</td></tr></table>				Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.
Option	Description											
<i>auto</i>	Set outgoing interface automatically.											
<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.											
<i>specify</i>	Set outgoing interface manually.											
interface	Specify outgoing interface to reach server.	string	Maximum length: 15									

## config user saml

SAML server entry configuration.

```

config user saml
    Description: SAML server entry configuration.
    edit <name>
        set adfs-claim [enable|disable]
        set cert {string}
        set clock-tolerance {integer}
        set digest-method [sha1|sha256]
        set entity-id {string}
        set group-claim-type [email|given-name|...]
        set group-name {string}
        set idp-cert {string}
        set idp-entity-id {string}
        set idp-single-logout-url {string}
        set idp-single-sign-on-url {string}
        set limit-relaystate [enable|disable]
        set single-logout-url {string}
        set single-sign-on-url {string}
        set user-claim-type [email|given-name|...]
        set user-name {string}
    next
end

```

## config user saml

Parameter	Description	Type	Size	Default
adfs-claim	Enable/disable ADFS Claim for user/group attribute in assertion statement.	option	-	disable

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable ADFS Claim for user/group attribute in assertion statement.		
	<i>disable</i>	Disable ADFS Claim for user/group attribute in assertion statement.		
cert	Certificate to sign SAML messages.	string	Maximum length: 35	
clock-tolerance	Clock skew tolerance in seconds.	integer	Minimum value: 0 Maximum value: 300	15
digest-method	Digest method algorithm.	option	-	sha1
	<b>Option</b>	<b>Description</b>		
	<i>sha1</i>	Digest Method Algorithm is SHA1.		
	<i>sha256</i>	Digest Method Algorithm is SHA256.		
entity-id	SP entity ID.	string	Maximum length: 255	
group-claim-type	Group claim in assertion statement.	option	-	group
	<b>Option</b>	<b>Description</b>		
	<i>email</i>	E-mail address of the user.		
	<i>given-name</i>	Given name of the user.		
	<i>name</i>	Unique name of the user.		
	<i>upn</i>	User principal name (UPN) of the user.		
	<i>common-name</i>	Common name of the user.		
	<i>email-adfs-1x</i>	E-mail address of the user when interoperating with AD FS 1.1 or ADFS 1.0.		
	<i>group</i>	Group that the user is a member of.		
	<i>upn-adfs-1x</i>	User principal name (UPN) of the user.		
	<i>role</i>	Role that the user has.		
	<i>sur-name</i>	Surname of the user		
	<i>ppid</i>	Private identifier of the user.		
	<i>name-identifier</i>	SAML name identifier of the user.		

Parameter	Description	Type	Size	Default																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>authentication-method</i></td><td>Method used to authenticate the user.</td></tr><tr><td><i>deny-only-group-sid</i></td><td>Deny-only group SID of the user.</td></tr><tr><td><i>deny-only-primary-sid</i></td><td>Deny-only primary SID of the user.</td></tr><tr><td><i>deny-only-primary-group-sid</i></td><td>Deny-only primary group SID of the user.</td></tr><tr><td><i>group-sid</i></td><td>Group SID of the user.</td></tr><tr><td><i>primary-group-sid</i></td><td>Primary group SID of the user.</td></tr><tr><td><i>primary-sid</i></td><td>Primary SID of the user.</td></tr><tr><td><i>windows-account-name</i></td><td>Domain account name of the user in the form of &lt;domain&gt;\&lt;user&gt;.</td></tr></table>	Option	Description	<i>authentication-method</i>	Method used to authenticate the user.	<i>deny-only-group-sid</i>	Deny-only group SID of the user.	<i>deny-only-primary-sid</i>	Deny-only primary SID of the user.	<i>deny-only-primary-group-sid</i>	Deny-only primary group SID of the user.	<i>group-sid</i>	Group SID of the user.	<i>primary-group-sid</i>	Primary group SID of the user.	<i>primary-sid</i>	Primary SID of the user.	<i>windows-account-name</i>	Domain account name of the user in the form of <domain>\<user>.			
	Option	Description																				
	<i>authentication-method</i>	Method used to authenticate the user.																				
	<i>deny-only-group-sid</i>	Deny-only group SID of the user.																				
	<i>deny-only-primary-sid</i>	Deny-only primary SID of the user.																				
	<i>deny-only-primary-group-sid</i>	Deny-only primary group SID of the user.																				
	<i>group-sid</i>	Group SID of the user.																				
	<i>primary-group-sid</i>	Primary group SID of the user.																				
	<i>primary-sid</i>	Primary SID of the user.																				
<i>windows-account-name</i>	Domain account name of the user in the form of <domain>\<user>.																					
group-name	Group name in assertion statement.	string	Maximum length: 255																			
idp-cert	IDP Certificate name.	string	Maximum length: 35																			
idp-entity-id	IDP entity ID.	string	Maximum length: 255																			
idp-single-logout-url	IDP single logout url.	string	Maximum length: 255																			
idp-single-sign-on-url	IDP single sign-on URL.	string	Maximum length: 255																			
limit-relaystate	Enable/disable limiting of relay-state parameter when it exceeds SAML 2.0 specification limits (80 bytes).	option	-	disable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable limiting of relay-state parameter when it exceeds SAML 2.0 specification limits (80 bytes).</td></tr><tr><td><i>disable</i></td><td>Disable limiting of relay-state parameter when it exceeds SAML 2.0 specification limits (80 bytes).</td></tr></table>	Option	Description	<i>enable</i>	Enable limiting of relay-state parameter when it exceeds SAML 2.0 specification limits (80 bytes).	<i>disable</i>	Disable limiting of relay-state parameter when it exceeds SAML 2.0 specification limits (80 bytes).															
	Option	Description																				
	<i>enable</i>	Enable limiting of relay-state parameter when it exceeds SAML 2.0 specification limits (80 bytes).																				
<i>disable</i>	Disable limiting of relay-state parameter when it exceeds SAML 2.0 specification limits (80 bytes).																					
name	SAML server entry name.	string	Maximum length: 35																			



Parameter	Description	Type	Size	Default
single-logout-url	SP single logout URL.	string	Maximum length: 255	
single-sign-on-url	SP single sign-on URL.	string	Maximum length: 255	
user-claim-type	User name claim in assertion statement.	option	-	upn

Option	Description
<i>email</i>	E-mail address of the user.
<i>given-name</i>	Given name of the user.
<i>name</i>	Unique name of the user.
<i>upn</i>	User principal name (UPN) of the user.
<i>common-name</i>	Common name of the user.
<i>email-adfs-1x</i>	E-mail address of the user when interoperating with AD FS 1.1 or ADFS 1.0.
<i>group</i>	Group that the user is a member of.
<i>upn-adfs-1x</i>	User principal name (UPN) of the user.
<i>role</i>	Role that the user has.
<i>sur-name</i>	Surname of the user
<i>ppid</i>	Private identifier of the user.
<i>name-identifier</i>	SAML name identifier of the user.
<i>authentication-method</i>	Method used to authenticate the user.
<i>deny-only-group-sid</i>	Deny-only group SID of the user.
<i>deny-only-primary-sid</i>	Deny-only primary SID of the user.
<i>deny-only-primary-group-sid</i>	Deny-only primary group SID of the user.
<i>group-sid</i>	Group SID of the user.
<i>primary-group-sid</i>	Primary group SID of the user.
<i>primary-sid</i>	Primary SID of the user.
<i>windows-account-name</i>	Domain account name of the user in the form of <domain>\<user>.

Parameter	Description	Type	Size	Default
user-name	User name in assertion statement.	string	Maximum length: 255	

## config user security-exempt-list

Configure security exemption list.

```
config user security-exempt-list
    Description: Configure security exemption list.
    edit <name>
        set description {string}
        config rule
            Description: Configure rules for exempting users from captive portal
authentication.
            edit <id>
                set srcaddr <name1>, <name2>, ...
                set dstaddr <name1>, <name2>, ...
                set service <name1>, <name2>, ...
            next
        end
    next
end
```

## config user security-exempt-list

Parameter	Description	Type	Size	Default
description	Description.	string	Maximum length: 127	
name	Name of the exempt list.	string	Maximum length: 35	

## config rule

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
srcaddr <name>	Source addresses or address groups. Address or group name.	string	Maximum length: 79	
dstaddr <name>	Destination addresses or address groups. Address or group name.	string	Maximum length: 79	

Parameter	Description	Type	Size	Default
service <name>	Destination services. Service name.	string	Maximum length: 79	

## config user setting

Configure user authentication setting.

```

config user setting
    Description: Configure user authentication setting.
    set auth-blackout-time {integer}
    set auth-ca-cert {string}
    set auth-cert {string}
    set auth-http-basic [enable|disable]
    set auth-invalid-max {integer}
    set auth-lockout-duration {integer}
    set auth-lockout-threshold {integer}
    set auth-on-demand [always|implicitly]
    set auth-portal-timeout {integer}
    config auth-ports
        Description: Set up non-standard ports for authentication with HTTP, HTTPS, FTP, and
        TELNET.
        edit <id>
            set type [http|https|...]
            set port {integer}
        next
    end
    set auth-secure-http [enable|disable]
    set auth-src-mac [enable|disable]
    set auth-ssl-allow-renegotiation [enable|disable]
    set auth-ssl-max-proto-version [ssl3|tlsv1|...]
    set auth-ssl-min-proto-version [default|SSLv3|...]
    set auth-ssl-sigalgs [no-rsa-pss|all]
    set auth-timeout {integer}
    set auth-timeout-type [idle-timeout|hard-timeout|...]
    set auth-type {option1}, {option2}, ...
    set per-policy-disclaimer [enable|disable]
    set radius-ses-timeout-act [hard-timeout|ignore-timeout]
end

```

## config user setting

Parameter	Description	Type	Size	Default
auth-blackout-time	Time in seconds an IP address is denied access after failing to authenticate five times within one minute.	integer	Minimum value: 0 Maximum value: 3600	0

Parameter	Description	Type	Size	Default						
auth-ca-cert	HTTPS CA certificate for policy authentication.	string	Maximum length: 35							
auth-cert	HTTPS server certificate for policy authentication.	string	Maximum length: 35							
auth-http-basic	Enable/disable use of HTTP basic authentication for identity-based firewall policies.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>				Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.
	Option	Description								
	<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.									
auth-invalid-max	Maximum number of failed authentication attempts before the user is blocked.	integer	Minimum value: 1 Maximum value: 100	5						
auth-lockout-duration	Lockout period in seconds after too many login failures.	integer	Minimum value: 0 Maximum value: 4294967295	0						
auth-lockout-threshold	Maximum number of failed login attempts before login lockout is triggered.	integer	Minimum value: 1 Maximum value: 10	3						
auth-on-demand	Always/implicitly trigger firewall authentication on demand.	option	-	implicitly						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>always</i></td><td>Always trigger firewall authentication on demand.</td></tr><tr><td><i>implicitly</i></td><td>Implicitly trigger firewall authentication on demand.</td></tr></table>				Option	Description	<i>always</i>	Always trigger firewall authentication on demand.	<i>implicitly</i>	Implicitly trigger firewall authentication on demand.
	Option	Description								
	<i>always</i>	Always trigger firewall authentication on demand.								
<i>implicitly</i>	Implicitly trigger firewall authentication on demand.									
auth-portal-timeout	Time in minutes before captive portal user have to re-authenticate.	integer	Minimum value: 1 Maximum value: 30	3						
auth-secure-http	Enable/disable redirecting HTTP user authentication to more secure HTTPS.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>				Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.
	Option	Description								
	<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.									

Parameter	Description	Type	Size	Default												
auth-src-mac	Enable/disable source MAC for user identity.	option	-	enable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable source MAC for user identity.</td></tr><tr><td><i>disable</i></td><td>Disable source MAC for user identity.</td></tr></table>	Option	Description	<i>enable</i>	Enable source MAC for user identity.	<i>disable</i>	Disable source MAC for user identity.									
Option	Description															
<i>enable</i>	Enable source MAC for user identity.															
<i>disable</i>	Disable source MAC for user identity.															
auth-ssl-allow-renegotiation	Allow/forbid SSL re-negotiation for HTTPS authentication.	option	-	disable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Allow SSL re-negotiation.</td></tr><tr><td><i>disable</i></td><td>Forbid SSL re-negotiation.</td></tr></table>	Option	Description	<i>enable</i>	Allow SSL re-negotiation.	<i>disable</i>	Forbid SSL re-negotiation.									
Option	Description															
<i>enable</i>	Allow SSL re-negotiation.															
<i>disable</i>	Forbid SSL re-negotiation.															
auth-ssl-max-proto-version	Maximum supported protocol version for SSL/TLS connections.	option	-													
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>sslV3</i></td><td>SSLv3.</td></tr><tr><td><i>tlsv1</i></td><td>TLSv1.</td></tr><tr><td><i>tlsv1-1</i></td><td>TLSv1.1.</td></tr><tr><td><i>tlsv1-2</i></td><td>TLSv1.2.</td></tr><tr><td><i>tlsv1-3</i></td><td>TLSv1.3.</td></tr></table>	Option	Description	<i>sslV3</i>	SSLv3.	<i>tlsv1</i>	TLSv1.	<i>tlsv1-1</i>	TLSv1.1.	<i>tlsv1-2</i>	TLSv1.2.	<i>tlsv1-3</i>	TLSv1.3.			
Option	Description															
<i>sslV3</i>	SSLv3.															
<i>tlsv1</i>	TLSv1.															
<i>tlsv1-1</i>	TLSv1.1.															
<i>tlsv1-2</i>	TLSv1.2.															
<i>tlsv1-3</i>	TLSv1.3.															
auth-ssl-min-proto-version	Minimum supported protocol version for SSL/TLS connections.	option	-	default												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>Follow system global setting.</td></tr><tr><td><i>SSLv3</i></td><td>SSLv3.</td></tr><tr><td><i>TLSv1</i></td><td>TLSv1.</td></tr><tr><td><i>TLSv1-1</i></td><td>TLSv1.1.</td></tr><tr><td><i>TLSv1-2</i></td><td>TLSv1.2.</td></tr></table>	Option	Description	<i>default</i>	Follow system global setting.	<i>SSLv3</i>	SSLv3.	<i>TLSv1</i>	TLSv1.	<i>TLSv1-1</i>	TLSv1.1.	<i>TLSv1-2</i>	TLSv1.2.			
Option	Description															
<i>default</i>	Follow system global setting.															
<i>SSLv3</i>	SSLv3.															
<i>TLSv1</i>	TLSv1.															
<i>TLSv1-1</i>	TLSv1.1.															
<i>TLSv1-2</i>	TLSv1.2.															
auth-ssl-sigalgs	Set signature algorithms related to HTTPS authentication.	option	-	all												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>no-rsa-pss</i></td><td>Disable RSA-PSS signature algorithms for HTTPS authentication.</td></tr><tr><td><i>all</i></td><td>Enable all supported signature algorithms for HTTPS authentication.</td></tr></table>	Option	Description	<i>no-rsa-pss</i>	Disable RSA-PSS signature algorithms for HTTPS authentication.	<i>all</i>	Enable all supported signature algorithms for HTTPS authentication.									
Option	Description															
<i>no-rsa-pss</i>	Disable RSA-PSS signature algorithms for HTTPS authentication.															
<i>all</i>	Enable all supported signature algorithms for HTTPS authentication.															

Parameter	Description	Type	Size	Default										
auth-timeout	Time in minutes before the firewall user authentication timeout requires the user to re-authenticate.	integer	Minimum value: 1 Maximum value: 1440	5										
auth-timeout-type	Control if authenticated users have to login again after a hard timeout, after an idle timeout, or after a session timeout.	option	-	idle-timeout										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>idle-timeout</i></td><td>Idle timeout.</td></tr><tr><td><i>hard-timeout</i></td><td>Hard timeout.</td></tr><tr><td><i>new-session</i></td><td>New session timeout.</td></tr></table>	Option	Description	<i>idle-timeout</i>	Idle timeout.	<i>hard-timeout</i>	Hard timeout.	<i>new-session</i>	New session timeout.					
Option	Description													
<i>idle-timeout</i>	Idle timeout.													
<i>hard-timeout</i>	Hard timeout.													
<i>new-session</i>	New session timeout.													
auth-type	Supported firewall policy authentication protocols/methods.	option	-	http https ftp telnet										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>http</i></td><td>Allow HTTP authentication.</td></tr><tr><td><i>https</i></td><td>Allow HTTPS authentication.</td></tr><tr><td><i>ftp</i></td><td>Allow FTP authentication.</td></tr><tr><td><i>telnet</i></td><td>Allow TELNET authentication.</td></tr></table>	Option	Description	<i>http</i>	Allow HTTP authentication.	<i>https</i>	Allow HTTPS authentication.	<i>ftp</i>	Allow FTP authentication.	<i>telnet</i>	Allow TELNET authentication.			
Option	Description													
<i>http</i>	Allow HTTP authentication.													
<i>https</i>	Allow HTTPS authentication.													
<i>ftp</i>	Allow FTP authentication.													
<i>telnet</i>	Allow TELNET authentication.													
per-policy-disclaimer	Enable/disable per policy disclaimer.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable per policy disclaimer.</td></tr><tr><td><i>disable</i></td><td>Disable per policy disclaimer.</td></tr></table>	Option	Description	<i>enable</i>	Enable per policy disclaimer.	<i>disable</i>	Disable per policy disclaimer.							
Option	Description													
<i>enable</i>	Enable per policy disclaimer.													
<i>disable</i>	Disable per policy disclaimer.													
radius-ses-timeout-act	Set the RADIUS session timeout to a hard timeout or to ignore RADIUS server session timeouts.	option	-	hard-timeout										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>hard-timeout</i></td><td>Use session timeout from RADIUS as hard-timeout.</td></tr><tr><td><i>ignore-timeout</i></td><td>Ignore session timeout from RADIUS.</td></tr></table>	Option	Description	<i>hard-timeout</i>	Use session timeout from RADIUS as hard-timeout.	<i>ignore-timeout</i>	Ignore session timeout from RADIUS.							
Option	Description													
<i>hard-timeout</i>	Use session timeout from RADIUS as hard-timeout.													
<i>ignore-timeout</i>	Ignore session timeout from RADIUS.													

## config auth-ports

Parameter	Description	Type	Size	Default										
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0										
type	Service type.	option	-	http										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>http</td><td>HTTP service.</td></tr><tr><td>https</td><td>HTTPS service.</td></tr><tr><td>ftp</td><td>FTP service.</td></tr><tr><td>telnet</td><td>TELNET service.</td></tr></table>				Option	Description	http	HTTP service.	https	HTTPS service.	ftp	FTP service.	telnet	TELNET service.
	Option	Description												
	http	HTTP service.												
	https	HTTPS service.												
	ftp	FTP service.												
telnet	TELNET service.													
port	Non-standard port for firewall user authentication.	integer	Minimum value: 1 Maximum value: 65535	1024										

## config user tacacs+

Configure TACACS+ server entries.

```
config user tacacs+
  Description: Configure TACACS+ server entries.
  edit <name>
    set authen-type [mschap|chap|...]
    set authorization [enable|disable]
    set interface {string}
    set interface-select-method [auto|sdwan|...]
    set key {password}
    set port {integer}
    set secondary-key {password}
    set secondary-server {string}
    set server {string}
    set source-ip {string}
    set tertiary-key {password}
    set tertiary-server {string}
  next
end
```

## config user tacacs+

Parameter	Description	Type	Size	Default												
authen-type	Allowed authentication protocols/methods.	option	-	auto												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>mschap</i></td><td>MSCHAP.</td></tr><tr><td><i>chap</i></td><td>CHAP.</td></tr><tr><td><i>pap</i></td><td>PAP.</td></tr><tr><td><i>ascii</i></td><td>ASCII.</td></tr><tr><td><i>auto</i></td><td>Use PAP, MSCHAP, and CHAP (in that order).</td></tr></table>	Option	Description	<i>mschap</i>	MSCHAP.	<i>chap</i>	CHAP.	<i>pap</i>	PAP.	<i>ascii</i>	ASCII.	<i>auto</i>	Use PAP, MSCHAP, and CHAP (in that order).			
	Option	Description														
	<i>mschap</i>	MSCHAP.														
	<i>chap</i>	CHAP.														
	<i>pap</i>	PAP.														
	<i>ascii</i>	ASCII.														
	<i>auto</i>	Use PAP, MSCHAP, and CHAP (in that order).														
authorization	Enable/disable TACACS+ authorization.	option	-	disable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable TACACS+ authorization.</td></tr><tr><td><i>disable</i></td><td>Disable TACACS+ authorization.</td></tr></table>	Option	Description	<i>enable</i>	Enable TACACS+ authorization.	<i>disable</i>	Disable TACACS+ authorization.									
	Option	Description														
	<i>enable</i>	Enable TACACS+ authorization.														
	<i>disable</i>	Disable TACACS+ authorization.														
interface	Specify outgoing interface to reach server.	string	Maximum length: 15													
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto</i></td><td>Set outgoing interface automatically.</td></tr><tr><td><i>sdwan</i></td><td>Set outgoing interface by SD-WAN or policy routing rules.</td></tr><tr><td><i>specify</i></td><td>Set outgoing interface manually.</td></tr></table>	Option	Description	<i>auto</i>	Set outgoing interface automatically.	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.	<i>specify</i>	Set outgoing interface manually.							
	Option	Description														
	<i>auto</i>	Set outgoing interface automatically.														
	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.														
<i>specify</i>	Set outgoing interface manually.															
key	Key to access the primary server.	password	Not Specified													
name	TACACS+ server entry name.	string	Maximum length: 35													
port	Port number of the TACACS+ server.	integer	Minimum value: 1 Maximum value: 65535	49												
secondary-key	Key to access the secondary server.	password	Not Specified													



Parameter	Description	Type	Size	Default
secondary-server	Secondary TACACS+ server CN domain name or IP address.	string	Maximum length: 63	
server	Primary TACACS+ server CN domain name or IP address.	string	Maximum length: 63	
source-ip	Source IP address for communications to TACACS+ server.	string	Maximum length: 63	
tertiary-key	Key to access the tertiary server.	password	Not Specified	
tertiary-server	Tertiary TACACS+ server CN domain name or IP address.	string	Maximum length: 63	

## videofilter

This section includes syntax for the following commands:

- [config videofilter profile on page 1630](#)
- [config videofilter youtube-channel-filter on page 1632](#)
- [config videofilter youtube-key on page 1634](#)

### config videofilter profile

Configure VideoFilter profile.

```
config videofilter profile
  Description: Configure VideoFilter profile.
  edit <name>
    set comment {var-string}
    set dailymotion [enable|disable]
    config fortiguard-category
      Description: Configure FortiGuard categories.
      config filters
        Description: Configure VideoFilter FortiGuard category.
        edit <id>
          set action [allow|monitor|...]
          set category-id {integer}
          set log [enable|disable]
        next
      end
    end
    set replacemsg-group {string}
    set vimeo [enable|disable]
    set youtube [enable|disable]
    set youtube-channel-filter {integer}
  next
end
```

### config videofilter profile

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 255	
dailymotion	Enable/disable Dailymotion video source.	option	-	enable
	<b>Option</b>		<b>Description</b>	
	<i>enable</i>		Enable Dailymotion source.	
	<i>disable</i>		Disable Dailymotion source.	

Parameter	Description	Type	Size	Default
name	Name.	string	Maximum length: 35	
replacemsg-group	Replacement message group.	string	Maximum length: 35	
vimeo	Enable/disable Vimeo video source.	option	-	enable
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Enable Vimeo source.		
	<i>disable</i>	Disable Vimeo source.		
youtube	Enable/disable YouTube video source.	option	-	enable
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Enable YouTube source.		
	<i>disable</i>	Disable YouTube source.		
youtube-channel-filter	Set YouTube channel filter.	integer	Minimum value: 0 Maximum value: 4294967295	0

### config filters

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
action	VideoFilter action.	option	-	monitor
	<b>Option</b> <b>Description</b>			
	<i>allow</i>	Allow videos to be accessed.		
	<i>monitor</i>	Monitor videos.		
	<i>block</i>	Block videos.		

Parameter	Description	Type	Size	Default
category-id	Category ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
log	Enable/disable logging.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable logging.		
	<i>disable</i>	Disable logging.		

## config videofilter youtube-channel-filter

Configure YouTube channel filter.

```

config videofilter youtube-channel-filter
  Description: Configure YouTube channel filter.
  edit <id>
    set comment {var-string}
    set default-action [allow|monitor|...]
    config entries
      Description: YouTube filter entries.
      edit <id>
        set comment {var-string}
        set action [allow|monitor|...]
        set channel-id {string}
      next
    end
  set log [enable|disable]
  set name {string}
  set override-category [enable|disable]
next
end

```

## config videofilter youtube-channel-filter

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 255	
default-action	YouTube channel filter default action.	option	-	monitor
	Option	Description		
	allow	Allow videos to be accessed.		

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>monitor</i>	Monitor videos.		
	<i>block</i>	Block videos.		
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
log	Enable/disable logging.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable logging.		
	<i>disable</i>	Disable logging.		
name	Name.	string	Maximum length: 35	
override-category	Enable/disable overriding category filtering result.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable overriding category filtering result.		
	<i>disable</i>	Disable overriding category filtering result.		

### config entries

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
comment	Comment.	var-string	Maximum length: 255	
action	YouTube channel filter action.	option	-	monitor
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow videos to be accessed.		

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>monitor</i>	Monitor videos.		
	<i>block</i>	Block videos.		
channel-id	Channel ID.	string	Maximum length: 255	

## config videofilter youtube-key

Configure YouTube API keys.

```
config videofilter youtube-key
    Description: Configure YouTube API keys.
    edit <id>
        set key {string}
    next
end
```

## config videofilter youtube-key

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
key	Key.	string	Maximum length: 47	

## voip

This section includes syntax for the following commands:

- [config voip profile on page 1635](#)

### config voip profile

Configure VoIP profiles.

```
config voip profile
  Description: Configure VoIP profiles.
  edit <name>
    set comment {var-string}
    set feature-set [flow|proxy]
    config msrp
      Description: MSRP.
      set status [disable|enable]
      set log-violations [disable|enable]
      set max-msg-size {integer}
      set max-msg-size-action [pass|block|...]
    end
    config sccp
      Description: SCCP.
      set status [disable|enable]
      set block-mcast [disable|enable]
      set verify-header [disable|enable]
      set log-call-summary [disable|enable]
      set log-violations [disable|enable]
      set max-calls {integer}
    end
    config sip
      Description: SIP.
      set status [disable|enable]
      set rtp [disable|enable]
      set nat-port-range {user}
      set open-register-pinhole [disable|enable]
      set open-contact-pinhole [disable|enable]
      set strict-register [disable|enable]
      set register-rate {integer}
      set register-rate-track [none|src-ip|...]
      set invite-rate {integer}
      set invite-rate-track [none|src-ip|...]
      set max-dialogs {integer}
      set max-line-length {integer}
      set block-long-lines [disable|enable]
      set block-unknown [disable|enable]
      set call-keepalive {integer}
      set block-ack [disable|enable]
      set block-bye [disable|enable]
      set block-cancel [disable|enable]
```

---

```
set block-info [disable|enable]
set block-invite [disable|enable]
set block-message [disable|enable]
set block-notify [disable|enable]
set block-options [disable|enable]
set block-prack [disable|enable]
set block-publish [disable|enable]
set block-refer [disable|enable]
set block-register [disable|enable]
set block-subscribe [disable|enable]
set block-update [disable|enable]
set register-contact-trace [disable|enable]
set open-via-pinhole [disable|enable]
set open-record-route-pinhole [disable|enable]
set rfc2543-branch [disable|enable]
set log-violations [disable|enable]
set log-call-summary [disable|enable]
set nat-trace [disable|enable]
set subscribe-rate {integer}
set subscribe-rate-track [none|src-ip|...]
set message-rate {integer}
set message-rate-track [none|src-ip|...]
set notify-rate {integer}
set notify-rate-track [none|src-ip|...]
set refer-rate {integer}
set refer-rate-track [none|src-ip|...]
set update-rate {integer}
set update-rate-track [none|src-ip|...]
set options-rate {integer}
set options-rate-track [none|src-ip|...]
set ack-rate {integer}
set ack-rate-track [none|src-ip|...]
set prack-rate {integer}
set prack-rate-track [none|src-ip|...]
set info-rate {integer}
set info-rate-track [none|src-ip|...]
set publish-rate {integer}
set publish-rate-track [none|src-ip|...]
set bye-rate {integer}
set bye-rate-track [none|src-ip|...]
set cancel-rate {integer}
set cancel-rate-track [none|src-ip|...]
set preserve-override [disable|enable]
set no-sdp-fixup [disable|enable]
set contact-fixup [disable|enable]
set max-idle-dialogs {integer}
set block-geo-red-options [disable|enable]
set hosted-nat-traversal [disable|enable]
set hnt-restrict-source-ip [disable|enable]
set max-body-length {integer}
set unknown-header [discard|pass|...]
set malformed-request-line [discard|pass|...]
set malformed-header-via [discard|pass|...]
set malformed-header-from [discard|pass|...]
set malformed-header-to [discard|pass|...]
set malformed-header-call-id [discard|pass|...]
```



```

set malformed-header-cseq [discard|pass|...]
set malformed-header-rack [discard|pass|...]
set malformed-header-rseq [discard|pass|...]
set malformed-header-contact [discard|pass|...]
set malformed-header-record-route [discard|pass|...]
set malformed-header-route [discard|pass|...]
set malformed-header-expires [discard|pass|...]
set malformed-header-content-type [discard|pass|...]
set malformed-header-content-length [discard|pass|...]
set malformed-header-max-forwards [discard|pass|...]
set malformed-header-allow [discard|pass|...]
set malformed-header-p-asserted-identity [discard|pass|...]
set malformed-header-no-require [discard|pass|...]
set malformed-header-no-proxy-require [discard|pass|...]
set malformed-header-sdp-v [discard|pass|...]
set malformed-header-sdp-o [discard|pass|...]
set malformed-header-sdp-s [discard|pass|...]
set malformed-header-sdp-i [discard|pass|...]
set malformed-header-sdp-c [discard|pass|...]
set malformed-header-sdp-b [discard|pass|...]
set malformed-header-sdp-z [discard|pass|...]
set malformed-header-sdp-k [discard|pass|...]
set malformed-header-sdp-a [discard|pass|...]
set malformed-header-sdp-t [discard|pass|...]
set malformed-header-sdp-r [discard|pass|...]
set malformed-header-sdp-m [discard|pass|...]
set provisional-invite-expiry-time {integer}
set ips-rtsp [disable|enable]
set ssl-mode [off|full]
set ssl-send-empty-frags [enable|disable]
set ssl-client-renegotiation [allow|deny|...]
set ssl-algorithm [high|medium|...]
set ssl-pfs [require|deny|...]
set ssl-min-version [ssl-3.0|tls-1.0|...]
set ssl-max-version [ssl-3.0|tls-1.0|...]
set ssl-client-certificate {string}
set ssl-server-certificate {string}
set ssl-auth-client {string}
set ssl-auth-server {string}
end
next
end

```

## config voip profile

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 255	
feature-set	Flow or proxy inspection feature set.	option	-	proxy

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>flow</i>	Flow feature set.		
	<i>proxy</i>	Proxy feature set.		
name	Profile name.	string	Maximum length: 35	

### config msrp

Parameter	Description	Type	Size	Default
status	Enable/disable MSRP.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
log-violations	Enable/disable logging of MSRP violations.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
max-msg-size	Maximum allowable MSRP message size.	integer	Minimum value: 0 Maximum value: 65535	0
max-msg-size-action	Action for violation of max-msg-size.	option	-	pass
	<b>Option</b>	<b>Description</b>		
	<i>pass</i>	Pass or allow matching traffic.		
	<i>block</i>	Block or drop matching traffic.		
	<i>reset</i>	Reset sessions for matching traffic.		
	<i>monitor</i>	Pass and log matching traffic.		

## config sccp

Parameter	Description	Type	Size	Default
status	Enable/disable SCCP.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
block-mcast	Enable/disable block multicast RTP connections.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
verify-header	Enable/disable verify SCCP header content.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
log-call-summary	Enable/disable log summary of SCCP calls.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
log-violations	Enable/disable logging of SCCP violations.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
max-calls	Maximum calls per minute per SCCP client (max 65535).	integer	Minimum value: 0 Maximum value: 65535	0

## config sip

Parameter	Description	Type	Size	Default						
status	Enable/disable SIP.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable status.</td></tr><tr><td><i>enable</i></td><td>Enable status.</td></tr></table>	Option	Description	<i>disable</i>	Disable status.	<i>enable</i>	Enable status.			
Option	Description									
<i>disable</i>	Disable status.									
<i>enable</i>	Enable status.									
rtp	Enable/disable create pinholes for RTP traffic to traverse firewall.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable status.</td></tr><tr><td><i>enable</i></td><td>Enable status.</td></tr></table>	Option	Description	<i>disable</i>	Disable status.	<i>enable</i>	Enable status.			
Option	Description									
<i>disable</i>	Disable status.									
<i>enable</i>	Enable status.									
nat-port-range	RTP NAT port range.	user	Not Specified	5117-65533						
open-register-pinhole	Enable/disable open pinhole for REGISTER Contact port.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable status.</td></tr><tr><td><i>enable</i></td><td>Enable status.</td></tr></table>	Option	Description	<i>disable</i>	Disable status.	<i>enable</i>	Enable status.			
Option	Description									
<i>disable</i>	Disable status.									
<i>enable</i>	Enable status.									
open-contact-pinhole	Enable/disable open pinhole for non-REGISTER Contact port.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable status.</td></tr><tr><td><i>enable</i></td><td>Enable status.</td></tr></table>	Option	Description	<i>disable</i>	Disable status.	<i>enable</i>	Enable status.			
Option	Description									
<i>disable</i>	Disable status.									
<i>enable</i>	Enable status.									
strict-register	Enable/disable only allow the registrar to connect.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable status.</td></tr><tr><td><i>enable</i></td><td>Enable status.</td></tr></table>	Option	Description	<i>disable</i>	Disable status.	<i>enable</i>	Enable status.			
Option	Description									
<i>disable</i>	Disable status.									
<i>enable</i>	Enable status.									
register-rate	REGISTER request rate limit (per second, per policy).	integer	Minimum value: 0 Maximum value: 4294967295	0						

Parameter	Description	Type	Size	Default								
register-rate-track	Track the packet protocol field.	option	-	none								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>None.</td></tr><tr><td><i>src-ip</i></td><td>Source IP.</td></tr><tr><td><i>dest-ip</i></td><td>Destination IP.</td></tr></table>	Option	Description	<i>none</i>	None.	<i>src-ip</i>	Source IP.	<i>dest-ip</i>	Destination IP.			
Option	Description											
<i>none</i>	None.											
<i>src-ip</i>	Source IP.											
<i>dest-ip</i>	Destination IP.											
invite-rate	INVITE request rate limit (per second, per policy).	integer	Minimum value: 0 Maximum value: 4294967295	0								
invite-rate-track	Track the packet protocol field.	option	-	none								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>None.</td></tr><tr><td><i>src-ip</i></td><td>Source IP.</td></tr><tr><td><i>dest-ip</i></td><td>Destination IP.</td></tr></table>	Option	Description	<i>none</i>	None.	<i>src-ip</i>	Source IP.	<i>dest-ip</i>	Destination IP.			
Option	Description											
<i>none</i>	None.											
<i>src-ip</i>	Source IP.											
<i>dest-ip</i>	Destination IP.											
max-dialogs	Maximum number of concurrent calls/dialogs (per policy).	integer	Minimum value: 0 Maximum value: 4294967295	0								
max-line-length	Maximum SIP header line length.	integer	Minimum value: 78 Maximum value: 4096	998								
block-long-lines	Enable/disable block requests with headers exceeding max-line-length.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable status.</td></tr><tr><td><i>enable</i></td><td>Enable status.</td></tr></table>	Option	Description	<i>disable</i>	Disable status.	<i>enable</i>	Enable status.					
Option	Description											
<i>disable</i>	Disable status.											
<i>enable</i>	Enable status.											
block-unknown	Block unrecognized SIP requests.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable status.</td></tr></table>	Option	Description	<i>disable</i>	Disable status.							
Option	Description											
<i>disable</i>	Disable status.											

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable status.		
call-keepalive	Continue tracking calls with no RTP for this many minutes.	integer	Minimum value: 0 Maximum value: 10080	0
block-ack	Enable/disable block ACK requests.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
block-bye	Enable/disable block BYE requests.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
block-cancel	Enable/disable block CANCEL requests.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
block-info	Enable/disable block INFO requests.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
block-invite	Enable/disable block INVITE requests.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
block-message	Enable/disable block MESSAGE requests.	option	-	disable

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
block-notify	Enable/disable block NOTIFY requests.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
block-options	Enable/disable block OPTIONS requests and no OPTIONS as notifying message for redundancy either.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
block-prack	Enable/disable block prack requests.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
block-publish	Enable/disable block PUBLISH requests.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
block-refer	Enable/disable block REFER requests.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
block-register	Enable/disable block REGISTER requests.	option	-	disable

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
block-subscribe	Enable/disable block SUBSCRIBE requests.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
block-update	Enable/disable block UPDATE requests.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
register-contact-trace	Enable/disable trace original IP/port within the contact header of REGISTER requests.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
open-via-pinhole	Enable/disable open pinhole for Via port.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
open-record-route-pinhole	Enable/disable open pinhole for Record-Route port.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
rfc2543-branch	Enable/disable support via branch compliant with RFC 2543.	option	-	disable



Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
log-violations	Enable/disable logging of SIP violations.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
log-call-summary	Enable/disable logging of SIP call summary.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
nat-trace	Enable/disable preservation of original IP in SDP i line.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
subscribe-rate	SUBSCRIBE request rate limit (per second, per policy).	integer	Minimum value: 0 Maximum value: 4294967295	0
subscribe-rate-track	Track the packet protocol field.	option	-	none
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	None.		
	<i>src-ip</i>	Source IP.		
	<i>dest-ip</i>	Destination IP.		

Parameter	Description	Type	Size	Default								
message-rate	MESSAGE request rate limit (per second, per policy).	integer	Minimum value: 0 Maximum value: 4294967295	0								
message-rate-track	Track the packet protocol field.	option	-	none								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>None.</td></tr><tr><td><i>src-ip</i></td><td>Source IP.</td></tr><tr><td><i>dest-ip</i></td><td>Destination IP.</td></tr></table>	Option	Description	<i>none</i>	None.	<i>src-ip</i>	Source IP.	<i>dest-ip</i>	Destination IP.			
Option	Description											
<i>none</i>	None.											
<i>src-ip</i>	Source IP.											
<i>dest-ip</i>	Destination IP.											
notify-rate	NOTIFY request rate limit (per second, per policy).	integer	Minimum value: 0 Maximum value: 4294967295	0								
notify-rate-track	Track the packet protocol field.	option	-	none								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>None.</td></tr><tr><td><i>src-ip</i></td><td>Source IP.</td></tr><tr><td><i>dest-ip</i></td><td>Destination IP.</td></tr></table>	Option	Description	<i>none</i>	None.	<i>src-ip</i>	Source IP.	<i>dest-ip</i>	Destination IP.			
Option	Description											
<i>none</i>	None.											
<i>src-ip</i>	Source IP.											
<i>dest-ip</i>	Destination IP.											
refer-rate	REFER request rate limit (per second, per policy).	integer	Minimum value: 0 Maximum value: 4294967295	0								
refer-rate-track	Track the packet protocol field.	option	-	none								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>None.</td></tr><tr><td><i>src-ip</i></td><td>Source IP.</td></tr><tr><td><i>dest-ip</i></td><td>Destination IP.</td></tr></table>	Option	Description	<i>none</i>	None.	<i>src-ip</i>	Source IP.	<i>dest-ip</i>	Destination IP.			
Option	Description											
<i>none</i>	None.											
<i>src-ip</i>	Source IP.											
<i>dest-ip</i>	Destination IP.											

Parameter	Description	Type	Size	Default								
update-rate	UPDATE request rate limit (per second, per policy).	integer	Minimum value: 0 Maximum value: 4294967295	0								
update-rate-track	Track the packet protocol field.	option	-	none								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>None.</td></tr><tr><td><i>src-ip</i></td><td>Source IP.</td></tr><tr><td><i>dest-ip</i></td><td>Destination IP.</td></tr></table>	Option	Description	<i>none</i>	None.	<i>src-ip</i>	Source IP.	<i>dest-ip</i>	Destination IP.			
Option	Description											
<i>none</i>	None.											
<i>src-ip</i>	Source IP.											
<i>dest-ip</i>	Destination IP.											
options-rate	OPTIONS request rate limit (per second, per policy).	integer	Minimum value: 0 Maximum value: 4294967295	0								
options-rate-track	Track the packet protocol field.	option	-	none								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>None.</td></tr><tr><td><i>src-ip</i></td><td>Source IP.</td></tr><tr><td><i>dest-ip</i></td><td>Destination IP.</td></tr></table>	Option	Description	<i>none</i>	None.	<i>src-ip</i>	Source IP.	<i>dest-ip</i>	Destination IP.			
Option	Description											
<i>none</i>	None.											
<i>src-ip</i>	Source IP.											
<i>dest-ip</i>	Destination IP.											
ack-rate	ACK request rate limit (per second, per policy).	integer	Minimum value: 0 Maximum value: 4294967295	0								
ack-rate-track	Track the packet protocol field.	option	-	none								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>None.</td></tr><tr><td><i>src-ip</i></td><td>Source IP.</td></tr><tr><td><i>dest-ip</i></td><td>Destination IP.</td></tr></table>	Option	Description	<i>none</i>	None.	<i>src-ip</i>	Source IP.	<i>dest-ip</i>	Destination IP.			
Option	Description											
<i>none</i>	None.											
<i>src-ip</i>	Source IP.											
<i>dest-ip</i>	Destination IP.											

Parameter	Description	Type	Size	Default								
prack-rate	PRACK request rate limit (per second, per policy).	integer	Minimum value: 0 Maximum value: 4294967295	0								
prack-rate-track	Track the packet protocol field.	option	-	none								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>None.</td></tr><tr><td><i>src-ip</i></td><td>Source IP.</td></tr><tr><td><i>dest-ip</i></td><td>Destination IP.</td></tr></table>	Option	Description	<i>none</i>	None.	<i>src-ip</i>	Source IP.	<i>dest-ip</i>	Destination IP.			
Option	Description											
<i>none</i>	None.											
<i>src-ip</i>	Source IP.											
<i>dest-ip</i>	Destination IP.											
info-rate	INFO request rate limit (per second, per policy).	integer	Minimum value: 0 Maximum value: 4294967295	0								
info-rate-track	Track the packet protocol field.	option	-	none								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>None.</td></tr><tr><td><i>src-ip</i></td><td>Source IP.</td></tr><tr><td><i>dest-ip</i></td><td>Destination IP.</td></tr></table>	Option	Description	<i>none</i>	None.	<i>src-ip</i>	Source IP.	<i>dest-ip</i>	Destination IP.			
Option	Description											
<i>none</i>	None.											
<i>src-ip</i>	Source IP.											
<i>dest-ip</i>	Destination IP.											
publish-rate	PUBLISH request rate limit (per second, per policy).	integer	Minimum value: 0 Maximum value: 4294967295	0								
publish-rate-track	Track the packet protocol field.	option	-	none								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>None.</td></tr><tr><td><i>src-ip</i></td><td>Source IP.</td></tr><tr><td><i>dest-ip</i></td><td>Destination IP.</td></tr></table>	Option	Description	<i>none</i>	None.	<i>src-ip</i>	Source IP.	<i>dest-ip</i>	Destination IP.			
Option	Description											
<i>none</i>	None.											
<i>src-ip</i>	Source IP.											
<i>dest-ip</i>	Destination IP.											

Parameter	Description	Type	Size	Default
bye-rate	BYE request rate limit (per second, per policy).	integer	Minimum value: 0 Maximum value: 4294967295	0
bye-rate-track	Track the packet protocol field.	option	-	none
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	None.		
	<i>src-ip</i>	Source IP.		
	<i>dest-ip</i>	Destination IP.		
cancel-rate	CANCEL request rate limit (per second, per policy).	integer	Minimum value: 0 Maximum value: 4294967295	0
cancel-rate-track	Track the packet protocol field.	option	-	none
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	None.		
	<i>src-ip</i>	Source IP.		
	<i>dest-ip</i>	Destination IP.		
preserve-override	Override i line to preserve original IPS.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
no-sdp-fixup	Enable/disable no SDP fix-up.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
contact-fixup	Fixup contact anyway even if contact's IP:port doesn't match session's IP:port.	option	-	enable

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
max-idle-dialogs	Maximum number established but idle dialogs to retain (per policy).	integer	Minimum value: 0 Maximum value: 4294967295	0
block-geo-red-options	Enable/disable block OPTIONS requests, but OPTIONS requests still notify for redundancy.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
hosted-nat-traversal	Hosted NAT Traversal (HNT).	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
hnt-restrict-source-ip	Enable/disable restrict RTP source IP to be the same as SIP source IP when HNT is enabled.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
max-body-length	Maximum SIP message body length (0 meaning no limit).	integer	Minimum value: 0 Maximum value: 4294967295	0
unknown-header	Action for unknown SIP header.	option	-	pass
	<b>Option</b>	<b>Description</b>		
	<i>discard</i>	Discard malformed messages.		

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>pass</i>	Bypass malformed messages.		
	<i>respond</i>	Respond with error code.		
malformed-request-line	Action for malformed request line.	option	-	pass
	<b>Option</b>	<b>Description</b>		
	<i>discard</i>	Discard malformed messages.		
	<i>pass</i>	Bypass malformed messages.		
	<i>respond</i>	Respond with error code.		
malformed-header-via	Action for malformed VIA header.	option	-	pass
	<b>Option</b>	<b>Description</b>		
	<i>discard</i>	Discard malformed messages.		
	<i>pass</i>	Bypass malformed messages.		
	<i>respond</i>	Respond with error code.		
malformed-header-from	Action for malformed From header.	option	-	pass
	<b>Option</b>	<b>Description</b>		
	<i>discard</i>	Discard malformed messages.		
	<i>pass</i>	Bypass malformed messages.		
	<i>respond</i>	Respond with error code.		
malformed-header-to	Action for malformed To header.	option	-	pass
	<b>Option</b>	<b>Description</b>		
	<i>discard</i>	Discard malformed messages.		
	<i>pass</i>	Bypass malformed messages.		
	<i>respond</i>	Respond with error code.		
malformed-header-call-id	Action for malformed Call-ID header.	option	-	pass

Parameter	Description	Type	Size	Default
	<b>Option</b> <b>Description</b>			
	<i>discard</i>	Discard malformed messages.		
	<i>pass</i>	Bypass malformed messages.		
	<i>respond</i>	Respond with error code.		
malformed-header-cseq	Action for malformed CSeq header.	option	-	pass
	<b>Option</b> <b>Description</b>			
	<i>discard</i>	Discard malformed messages.		
	<i>pass</i>	Bypass malformed messages.		
	<i>respond</i>	Respond with error code.		
malformed-header-rack	Action for malformed RACK header.	option	-	pass
	<b>Option</b> <b>Description</b>			
	<i>discard</i>	Discard malformed messages.		
	<i>pass</i>	Bypass malformed messages.		
	<i>respond</i>	Respond with error code.		
malformed-header-rseq	Action for malformed RSeq header.	option	-	pass
	<b>Option</b> <b>Description</b>			
	<i>discard</i>	Discard malformed messages.		
	<i>pass</i>	Bypass malformed messages.		
	<i>respond</i>	Respond with error code.		
malformed-header-contact	Action for malformed Contact header.	option	-	pass
	<b>Option</b> <b>Description</b>			
	<i>discard</i>	Discard malformed messages.		
	<i>pass</i>	Bypass malformed messages.		
	<i>respond</i>	Respond with error code.		
malformed-header-record-route	Action for malformed Record-Route header.	option	-	pass



Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>discard</i>	Discard malformed messages.		
	<i>pass</i>	Bypass malformed messages.		
	<i>respond</i>	Respond with error code.		
malformed-header-route	Action for malformed Route header.	option	-	pass
	<b>Option</b>	<b>Description</b>		
	<i>discard</i>	Discard malformed messages.		
	<i>pass</i>	Bypass malformed messages.		
	<i>respond</i>	Respond with error code.		
malformed-header-expires	Action for malformed Expires header.	option	-	pass
	<b>Option</b>	<b>Description</b>		
	<i>discard</i>	Discard malformed messages.		
	<i>pass</i>	Bypass malformed messages.		
	<i>respond</i>	Respond with error code.		
malformed-header-content-type	Action for malformed Content-Type header.	option	-	pass
	<b>Option</b>	<b>Description</b>		
	<i>discard</i>	Discard malformed messages.		
	<i>pass</i>	Bypass malformed messages.		
	<i>respond</i>	Respond with error code.		
malformed-header-content-length	Action for malformed Content-Length header.	option	-	pass
	<b>Option</b>	<b>Description</b>		
	<i>discard</i>	Discard malformed messages.		
	<i>pass</i>	Bypass malformed messages.		
	<i>respond</i>	Respond with error code.		

Parameter	Description	Type	Size	Default								
malformed-header-max-forwards	Action for malformed Max-Forwards header.	option	-	pass								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>discard</i></td><td>Discard malformed messages.</td></tr><tr><td><i>pass</i></td><td>Bypass malformed messages.</td></tr><tr><td><i>respond</i></td><td>Respond with error code.</td></tr></table>	Option	Description	<i>discard</i>	Discard malformed messages.	<i>pass</i>	Bypass malformed messages.	<i>respond</i>	Respond with error code.			
Option	Description											
<i>discard</i>	Discard malformed messages.											
<i>pass</i>	Bypass malformed messages.											
<i>respond</i>	Respond with error code.											
malformed-header-allow	Action for malformed Allow header.	option	-	pass								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>discard</i></td><td>Discard malformed messages.</td></tr><tr><td><i>pass</i></td><td>Bypass malformed messages.</td></tr><tr><td><i>respond</i></td><td>Respond with error code.</td></tr></table>	Option	Description	<i>discard</i>	Discard malformed messages.	<i>pass</i>	Bypass malformed messages.	<i>respond</i>	Respond with error code.			
Option	Description											
<i>discard</i>	Discard malformed messages.											
<i>pass</i>	Bypass malformed messages.											
<i>respond</i>	Respond with error code.											
malformed-header-p-asserted-identity	Action for malformed P-Asserted-Identity header.	option	-	pass								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>discard</i></td><td>Discard malformed messages.</td></tr><tr><td><i>pass</i></td><td>Bypass malformed messages.</td></tr><tr><td><i>respond</i></td><td>Respond with error code.</td></tr></table>	Option	Description	<i>discard</i>	Discard malformed messages.	<i>pass</i>	Bypass malformed messages.	<i>respond</i>	Respond with error code.			
Option	Description											
<i>discard</i>	Discard malformed messages.											
<i>pass</i>	Bypass malformed messages.											
<i>respond</i>	Respond with error code.											
malformed-header-no-require	Action for malformed SIP messages without Require header.	option	-	pass								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>discard</i></td><td>Discard malformed messages.</td></tr><tr><td><i>pass</i></td><td>Bypass malformed messages.</td></tr><tr><td><i>respond</i></td><td>Respond with error code.</td></tr></table>	Option	Description	<i>discard</i>	Discard malformed messages.	<i>pass</i>	Bypass malformed messages.	<i>respond</i>	Respond with error code.			
Option	Description											
<i>discard</i>	Discard malformed messages.											
<i>pass</i>	Bypass malformed messages.											
<i>respond</i>	Respond with error code.											
malformed-header-no-proxy-require	Action for malformed SIP messages without Proxy-Require header.	option	-	pass								

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>discard</i>	Discard malformed messages.		
	<i>pass</i>	Bypass malformed messages.		
	<i>respond</i>	Respond with error code.		
malformed-header-sdp-v	Action for malformed SDP v line.	option	-	pass
	<b>Option</b>	<b>Description</b>		
	<i>discard</i>	Discard malformed messages.		
	<i>pass</i>	Bypass malformed messages.		
	<i>respond</i>	Respond with error code.		
malformed-header-sdp-o	Action for malformed SDP o line.	option	-	pass
	<b>Option</b>	<b>Description</b>		
	<i>discard</i>	Discard malformed messages.		
	<i>pass</i>	Bypass malformed messages.		
	<i>respond</i>	Respond with error code.		
malformed-header-sdp-s	Action for malformed SDP s line.	option	-	pass
	<b>Option</b>	<b>Description</b>		
	<i>discard</i>	Discard malformed messages.		
	<i>pass</i>	Bypass malformed messages.		
	<i>respond</i>	Respond with error code.		
malformed-header-sdp-i	Action for malformed SDP i line.	option	-	pass
	<b>Option</b>	<b>Description</b>		
	<i>discard</i>	Discard malformed messages.		
	<i>pass</i>	Bypass malformed messages.		
	<i>respond</i>	Respond with error code.		
malformed-header-sdp-c	Action for malformed SDP c line.	option	-	pass

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>discard</i>	Discard malformed messages.		
	<i>pass</i>	Bypass malformed messages.		
	<i>respond</i>	Respond with error code.		
malformed-header-sdp-b	Action for malformed SDP b line.	option	-	pass
	<b>Option</b>	<b>Description</b>		
	<i>discard</i>	Discard malformed messages.		
	<i>pass</i>	Bypass malformed messages.		
	<i>respond</i>	Respond with error code.		
malformed-header-sdp-z	Action for malformed SDP z line.	option	-	pass
	<b>Option</b>	<b>Description</b>		
	<i>discard</i>	Discard malformed messages.		
	<i>pass</i>	Bypass malformed messages.		
	<i>respond</i>	Respond with error code.		
malformed-header-sdp-k	Action for malformed SDP k line.	option	-	pass
	<b>Option</b>	<b>Description</b>		
	<i>discard</i>	Discard malformed messages.		
	<i>pass</i>	Bypass malformed messages.		
	<i>respond</i>	Respond with error code.		
malformed-header-sdp-a	Action for malformed SDP a line.	option	-	pass
	<b>Option</b>	<b>Description</b>		
	<i>discard</i>	Discard malformed messages.		
	<i>pass</i>	Bypass malformed messages.		
	<i>respond</i>	Respond with error code.		
malformed-header-sdp-t	Action for malformed SDP t line.	option	-	pass

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>discard</i>	Discard malformed messages.		
	<i>pass</i>	Bypass malformed messages.		
	<i>respond</i>	Respond with error code.		
malformed-header-sdp-r	Action for malformed SDP r line.	option	-	pass
	<b>Option</b>	<b>Description</b>		
	<i>discard</i>	Discard malformed messages.		
	<i>pass</i>	Bypass malformed messages.		
	<i>respond</i>	Respond with error code.		
malformed-header-sdp-m	Action for malformed SDP m line.	option	-	pass
	<b>Option</b>	<b>Description</b>		
	<i>discard</i>	Discard malformed messages.		
	<i>pass</i>	Bypass malformed messages.		
	<i>respond</i>	Respond with error code.		
provisional-invite-expiry-time	Expiry time for provisional INVITE.	integer	Minimum value: 10 Maximum value: 3600	210
ips-rtp	Enable/disable allow IPS on RTP.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable status.		
	<i>enable</i>	Enable status.		
ssl-mode *	SSL/TLS mode for encryption & decryption of traffic.	option	-	off
	<b>Option</b>	<b>Description</b>		
	<i>off</i>	No SSL.		
	<i>full</i>	Client to FortiGate and FortiGate to Server SSL.		
ssl-send-empty-frags *	Send empty fragments to avoid attack on CBC IV (SSL 3.0 & TLS 1.0 only).	option	-	enable

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Send empty fragments.		
	<i>disable</i>	Do not send empty fragments.		
ssl-client-renegotiation *	Allow/block client renegotiation by server.	option	-	allow
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow a SSL client to renegotiate.		
	<i>deny</i>	Abort any SSL connection that attempts to renegotiate.		
	<i>secure</i>	Reject any SSL connection that does not offer a RFC 5746 Secure Renegotiation Indication.		
ssl-algorithm *	Relative strength of encryption algorithms accepted in negotiation.	option	-	high
	<b>Option</b>	<b>Description</b>		
	<i>high</i>	High encryption. Allow only AES and ChaCha.		
	<i>medium</i>	Medium encryption. Allow AES, ChaCha, 3DES, and RC4.		
	<i>low</i>	Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.		
ssl-pfs *	SSL Perfect Forward Secrecy.	option	-	allow
	<b>Option</b>	<b>Description</b>		
	<i>require</i>	PFS mandatory.		
	<i>deny</i>	PFS rejected.		
	<i>allow</i>	PFS allowed.		
ssl-min-version *	Lowest SSL/TLS version to negotiate.	option	-	tls-1.1
	<b>Option</b>	<b>Description</b>		
	<i>ssl-3.0</i>	SSL 3.0.		
	<i>tls-1.0</i>	TLS 1.0.		
	<i>tls-1.1</i>	TLS 1.1.		
	<i>tls-1.2</i>	TLS 1.2.		
	<i>tls-1.3</i>	TLS 1.3.		

Parameter	Description	Type	Size	Default												
ssl-max-version *	Highest SSL/TLS version to negotiate.	option	-	tls-1.3												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ssl-3.0</td><td>SSL 3.0.</td></tr><tr><td>tls-1.0</td><td>TLS 1.0.</td></tr><tr><td>tls-1.1</td><td>TLS 1.1.</td></tr><tr><td>tls-1.2</td><td>TLS 1.2.</td></tr><tr><td>tls-1.3</td><td>TLS 1.3.</td></tr></table>				Option	Description	ssl-3.0	SSL 3.0.	tls-1.0	TLS 1.0.	tls-1.1	TLS 1.1.	tls-1.2	TLS 1.2.	tls-1.3	TLS 1.3.
	Option	Description														
	ssl-3.0	SSL 3.0.														
	tls-1.0	TLS 1.0.														
	tls-1.1	TLS 1.1.														
	tls-1.2	TLS 1.2.														
tls-1.3	TLS 1.3.															
ssl-client-certificate *	Name of Certificate to offer to server if requested.	string	Maximum length: 35													
ssl-server-certificate *	Name of Certificate return to the client in every SSL connection.	string	Maximum length: 35													
ssl-auth-client *	Require a client certificate and authenticate it with the peer/peergrp.	string	Maximum length: 35													
ssl-auth-server *	Authenticate the server's certificate with the peer/peergrp.	string	Maximum length: 35													

\* This parameter may not exist in some models.

## vpn

This section includes syntax for the following commands:

- [config vpn certificate ca on page 1660](#)
- [config vpn certificate crl on page 1662](#)
- [config vpn certificate local on page 1663](#)
- [config vpn certificate ocsf-server on page 1667](#)
- [config vpn certificate remote on page 1668](#)
- [config vpn certificate setting on page 1668](#)
- [config vpn ipsec concentrator on page 1673](#)
- [config vpn ipsec fec on page 1674](#)
- [config vpn ipsec forticlient on page 1676](#)
- [config vpn ipsec manualkey-interface on page 1676](#)
- [config vpn ipsec manualkey on page 1679](#)
- [config vpn ipsec phase1-interface on page 1681](#)
- [config vpn ipsec phase1 on page 1706](#)
- [config vpn ipsec phase2-interface on page 1725](#)
- [config vpn ipsec phase2 on page 1735](#)
- [config vpn l2tp on page 1744](#)
- [config vpn ocvpn on page 1745](#)
- [config vpn pptp on page 1749](#)
- [config vpn ssl client on page 1750](#)
- [config vpn ssl settings on page 1752](#)
- [config vpn ssl web host-check-software on page 1765](#)
- [config vpn ssl web portal on page 1767](#)
- [config vpn ssl web realm on page 1786](#)
- [config vpn ssl web user-bookmark on page 1787](#)
- [config vpn ssl web user-group-bookmark on page 1794](#)

### config vpn certificate ca

CA certificate.

```
config vpn certificate ca
  Description: CA certificate.
  edit <name>
    set auto-update-days {integer}
    set auto-update-days-warning {integer}
    set ca {user}
    set ca-identifier {string}
    set range [global|vdom]
    set scep-url {string}
```



```

        set source [factory|user|...]
        set source-ip {ipv4-address}
        set ssl-inspection-trusted [enable|disable]
    next
end

```

## config vpn certificate ca

Parameter	Description	Type	Size	Default								
auto-update-days	Number of days to wait before requesting an updated CA certificate.	integer	Minimum value: 0 Maximum value: 4294967295	0								
auto-update-days-warning	Number of days before an expiry-warning message is generated.	integer	Minimum value: 0 Maximum value: 4294967295	0								
ca	CA certificate as a PEM file.	user	Not Specified									
ca-identifier	CA identifier of the SCEP server.	string	Maximum length: 255									
name	Name.	string	Maximum length: 79									
range	Either global or VDOM IP address range for the CA certificate.	option	-	vdom								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>global</i></td><td>Global range.</td></tr><tr><td><i>vdom</i></td><td>VDOM IP address range.</td></tr></table>				Option	Description	<i>global</i>	Global range.	<i>vdom</i>	VDOM IP address range.		
Option	Description											
<i>global</i>	Global range.											
<i>vdom</i>	VDOM IP address range.											
scep-url	URL of the SCEP server.	string	Maximum length: 255									
source	CA certificate source type.	option	-	user								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>factory</i></td><td>Factory installed certificate.</td></tr><tr><td><i>user</i></td><td>User generated certificate.</td></tr><tr><td><i>bundle</i></td><td>Bundle file certificate.</td></tr></table>				Option	Description	<i>factory</i>	Factory installed certificate.	<i>user</i>	User generated certificate.	<i>bundle</i>	Bundle file certificate.
Option	Description											
<i>factory</i>	Factory installed certificate.											
<i>user</i>	User generated certificate.											
<i>bundle</i>	Bundle file certificate.											
source-ip	Source IP address for communications to the SCEP server.	ipv4-address	Not Specified	0.0.0.0								

Parameter	Description	Type	Size	Default						
ssl-inspection-trusted	Enable/disable this CA as a trusted CA for SSL inspection.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Trusted CA for SSL inspection.</td></tr><tr><td><i>disable</i></td><td>Untrusted CA for SSL inspection.</td></tr></table>				Option	Description	<i>enable</i>	Trusted CA for SSL inspection.	<i>disable</i>	Untrusted CA for SSL inspection.
Option	Description									
<i>enable</i>	Trusted CA for SSL inspection.									
<i>disable</i>	Untrusted CA for SSL inspection.									

## config vpn certificate crl

Certificate Revocation List as a PEM file.

```

config vpn certificate crl
    Description: Certificate Revocation List as a PEM file.
    edit <name>
        set crl {user}
        set http-url {string}
        set ldap-password {password}
        set ldap-server {string}
        set ldap-username {string}
        set range [global|vdom]
        set scep-cert {string}
        set scep-url {string}
        set source [factory|user|...]
        set source-ip {ipv4-address}
        set update-interval {integer}
        set update-vdom {string}
    next
end

```

## config vpn certificate crl

Parameter	Description	Type	Size	Default
crl	Certificate Revocation List as a PEM file.	user	Not Specified	
http-url	HTTP server URL for CRL auto-update.	string	Maximum length: 255	
ldap-password	LDAP server user password.	password	Not Specified	
ldap-server	LDAP server name for CRL auto-update.	string	Maximum length: 35	
ldap-username	LDAP server user name.	string	Maximum length: 63	

Parameter	Description	Type	Size	Default								
name	Name.	string	Maximum length: 35									
range	Either global or VDOM IP address range for the certificate.	option	-	vdom								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>global</i></td><td>Global range.</td></tr><tr><td><i>vdom</i></td><td>VDOM IP address range.</td></tr></table>	Option	Description	<i>global</i>	Global range.	<i>vdom</i>	VDOM IP address range.					
Option	Description											
<i>global</i>	Global range.											
<i>vdom</i>	VDOM IP address range.											
scep-cert	Local certificate for SCEP communication for CRL auto-update.	string	Maximum length: 35	Fortinet_CA_SSL								
scep-url	SCEP server URL for CRL auto-update.	string	Maximum length: 255									
source	Certificate source type.	option	-	user								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>factory</i></td><td>Factory installed certificate.</td></tr><tr><td><i>user</i></td><td>User generated certificate.</td></tr><tr><td><i>bundle</i></td><td>Bundle file certificate.</td></tr></table>	Option	Description	<i>factory</i>	Factory installed certificate.	<i>user</i>	User generated certificate.	<i>bundle</i>	Bundle file certificate.			
Option	Description											
<i>factory</i>	Factory installed certificate.											
<i>user</i>	User generated certificate.											
<i>bundle</i>	Bundle file certificate.											
source-ip	Source IP address for communications to a HTTP or SCEP CA server.	ipv4-address	Not Specified	0.0.0.0								
update-interval	Time in seconds before the FortiGate checks for an updated CRL. Set to 0 to update only when it expires.	integer	Minimum value: 0 Maximum value: 4294967295	0								
update-vdom	VDOM for CRL update.	string	Maximum length: 31	root								

## config vpn certificate local

Local keys and certificates.

```
config vpn certificate local
    Description: Local keys and certificates.
    edit <name>
        set acme-ca-url {string}
        set acme-domain {string}
        set acme-email {string}
        set acme-renew-window {integer}
        set acme-rsa-key-size {integer}
        set auto-regenerate-days {integer}
```

```

set auto-regenerate-days-warning {integer}
set ca-identifier {string}
set certificate {user}
set cmp-path {string}
set cmp-regeneration-method [keyupdate|renewal]
set cmp-server {string}
set cmp-server-cert {string}
set comments {string}
set csr {user}
set enroll-protocol [none|scep|...]
set ike-localid {string}
set ike-localid-type [asn1dn|fqdn]
set name-encoding [printable|utf8]
set password {password}
set private-key {user}
set range [global|vdom]
set scep-password {password}
set scep-url {string}
set source [factory|user|...]
set source-ip {ipv4-address}
set state {user}
next
end

```

## config vpn certificate local

Parameter	Description	Type	Size	Default
acme-ca-url	The URL for the ACME CA server.	string	Maximum length: 255	https://acme-v02.api.letsencrypt.org/directory
acme-domain	A valid domain that resolves to this FortiGate unit.	string	Maximum length: 255	
acme-email	Contact email address that is required by some CAs like LetsEncrypt.	string	Maximum length: 255	
acme-renew-window	Beginning of the renewal window.	integer	Minimum value: 1 Maximum value: 100	30
acme-rsa-key-size	Length of the RSA private key of the generated cert (Minimum 2048 bits).	integer	Minimum value: 2048 Maximum value: 4096	2048
auto-regenerate-days	Number of days to wait before expiry of an updated local certificate is requested (0 = disabled).	integer	Minimum value: 0 Maximum value: 4294967295	0

Parameter	Description	Type	Size	Default										
auto-regenerate-days-warning	Number of days to wait before an expiry warning message is generated (0 = disabled).	integer	Minimum value: 0 Maximum value: 4294967295	0										
ca-identifier	CA identifier of the CA server for signing via SCEP.	string	Maximum length: 255											
certificate	PEM format certificate.	user	Not Specified											
cmp-path	Path location inside CMP server.	string	Maximum length: 255											
cmp-regeneration-method	CMP auto-regeneration method.	option	-	keyupate										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>keyupate</td><td>Key Update.</td></tr><tr><td>renewal</td><td>Renewal.</td></tr></table>				Option	Description	keyupate	Key Update.	renewal	Renewal.				
Option	Description													
keyupate	Key Update.													
renewal	Renewal.													
cmp-server	Address and port for CMP server (format = address:port).	string	Maximum length: 63											
cmp-server-cert	CMP server certificate.	string	Maximum length: 79											
comments	Comment.	string	Maximum length: 511											
csr	Certificate Signing Request.	user	Not Specified											
enroll-protocol	Certificate enrollment protocol.	option	-	none										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>none</td><td>None (default).</td></tr><tr><td>scep</td><td>Simple Certificate Enrollment Protocol.</td></tr><tr><td>cmpv2</td><td>Certificate Management Protocol Version 2.</td></tr><tr><td>acme2</td><td>Automated Certificate Management Environment Version 2.</td></tr></table>				Option	Description	none	None (default).	scep	Simple Certificate Enrollment Protocol.	cmpv2	Certificate Management Protocol Version 2.	acme2	Automated Certificate Management Environment Version 2.
Option	Description													
none	None (default).													
scep	Simple Certificate Enrollment Protocol.													
cmpv2	Certificate Management Protocol Version 2.													
acme2	Automated Certificate Management Environment Version 2.													
ike-localid	Local ID the FortiGate uses for authentication as a VPN client.	string	Maximum length: 63											
ike-localid-type	IKE local ID type.	option	-	asn1dn										

Parameter	Description	Type	Size	Default
	<b>Option</b> <b>Description</b>			
	<i>asn1dn</i>	ASN.1 distinguished name.		
	<i>fqdn</i>	Fully qualified domain name.		
name	Name.	string	Maximum length: 35	
name-encoding	Name encoding method for auto-regeneration.	option	-	printable
	<b>Option</b> <b>Description</b>			
	<i>printable</i>	Printable encoding (default).		
	<i>utf8</i>	UTF-8 encoding.		
password	Password as a PEM file.	password	Not Specified	
private-key	PEM format key encrypted with a password.	user	Not Specified	
range	Either a global or VDOM IP address range for the certificate.	option	-	vdom
	<b>Option</b> <b>Description</b>			
	<i>global</i>	Global range.		
	<i>vdom</i>	VDOM IP address range.		
scep-password	SCEP server challenge password for auto-regeneration.	password	Not Specified	
scep-url	SCEP server URL.	string	Maximum length: 255	
source	Certificate source type.	option	-	user
	<b>Option</b> <b>Description</b>			
	<i>factory</i>	Factory installed certificate.		
	<i>user</i>	User generated certificate.		
	<i>bundle</i>	Bundle file certificate.		
source-ip	Source IP address for communications to the SCEP server.	ipv4-address	Not Specified	0.0.0.0

Parameter	Description	Type	Size	Default
state	Certificate Signing Request State.	user	Not Specified	

## config vpn certificate ocsdp-server

OCSP server configuration.

```

config vpn certificate ocsdp-server
    Description: OCSP server configuration.
    edit <name>
        set cert {string}
        set secondary-cert {string}
        set secondary-url {string}
        set source-ip {ipv4-address}
        set unavail-action [revoke|ignore]
        set url {string}
    next
end

```

## config vpn certificate ocsdp-server

Parameter	Description	Type	Size	Default						
cert	OCSP server certificate.	string	Maximum length: 127							
name	OCSP server entry name.	string	Maximum length: 35							
secondary-cert	Secondary OCSP server certificate.	string	Maximum length: 127							
secondary-url	Secondary OCSP server URL.	string	Maximum length: 127							
source-ip	Source IP address for communications to the OCSP server.	ipv4-address	Not Specified	0.0.0.0						
unavail-action	Action when server is unavailable (revoke the certificate or ignore the result of the check).	option	-	revoke						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>revoke</i></td><td>Revoke certificate if server is unavailable.</td></tr><tr><td><i>ignore</i></td><td>Ignore OCSP check if server is unavailable.</td></tr></table>				Option	Description	<i>revoke</i>	Revoke certificate if server is unavailable.	<i>ignore</i>	Ignore OCSP check if server is unavailable.
Option	Description									
<i>revoke</i>	Revoke certificate if server is unavailable.									
<i>ignore</i>	Ignore OCSP check if server is unavailable.									
url	OCSP server URL.	string	Maximum length: 127							

## config vpn certificate remote

Remote certificate as a PEM file.

```
config vpn certificate remote
  Description: Remote certificate as a PEM file.
  edit <name>
    set range [global|vdom]
    set remote {user}
    set source [factory|user|...]
  next
end
```

## config vpn certificate remote

Parameter	Description	Type	Size	Default								
name	Name.	string	Maximum length: 35									
range	Either the global or VDOM IP address range for the remote certificate.	option	-	vdom								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>global</i></td><td>Global range.</td></tr><tr><td><i>vdom</i></td><td>VDOM IP address range.</td></tr></table>	Option	Description	<i>global</i>	Global range.	<i>vdom</i>	VDOM IP address range.					
Option	Description											
<i>global</i>	Global range.											
<i>vdom</i>	VDOM IP address range.											
remote	Remote certificate.	user	Not Specified									
source	Remote certificate source type.	option	-	user								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>factory</i></td><td>Factory installed certificate.</td></tr><tr><td><i>user</i></td><td>User generated certificate.</td></tr><tr><td><i>bundle</i></td><td>Bundle file certificate.</td></tr></table>	Option	Description	<i>factory</i>	Factory installed certificate.	<i>user</i>	User generated certificate.	<i>bundle</i>	Bundle file certificate.			
Option	Description											
<i>factory</i>	Factory installed certificate.											
<i>user</i>	User generated certificate.											
<i>bundle</i>	Bundle file certificate.											

## config vpn certificate setting

VPN certificate setting.

```
config vpn certificate setting
  Description: VPN certificate setting.
  set certname-dsa1024 {string}
  set certname-dsa2048 {string}
  set certname-ecdsa256 {string}
  set certname-ecdsa384 {string}
  set certname-ecdsa521 {string}
  set certname-ed25519 {string}
```



```

set certname-ed448 {string}
set certname-rsa1024 {string}
set certname-rsa2048 {string}
set certname-rsa4096 {string}
set check-ca-cert [enable|disable]
set check-ca-chain [enable|disable]
set cmp-key-usage-checking [enable|disable]
set cmp-save-extra-certs [enable|disable]
set cn-allow-multi [disable|enable]
set cn-match [substring|value]
config crt-verification
    Description: CRL verification options.
    set expiry [ignore|revoke]
    set leaf-crl-absence [ignore|revoke]
    set chain-crl-absence [ignore|revoke]
end
set interface {string}
set interface-select-method [auto|sdwan|...]
set ocsf-default-server {string}
set ocsf-option [certificate|server]
set ocsf-status [enable|disable]
set ssl-min-protoversion [default|SSLv3|...]
set ssl-ocsf-source-ip {ipv4-address}
set strict-ocsf-check [enable|disable]
set subject-match [substring|value]
set subject-set [subset|superset]
end

```

## config vpn certificate setting

Parameter	Description	Type	Size	Default
certname-dsa1024	1024 bit DSA key certificate for re-signing server certificates for SSL inspection.	string	Maximum length: 35	Fortinet_SSL_DSA1024
certname-dsa2048	2048 bit DSA key certificate for re-signing server certificates for SSL inspection.	string	Maximum length: 35	Fortinet_SSL_DSA2048
certname-ecdsa256	256 bit ECDSA key certificate for re-signing server certificates for SSL inspection.	string	Maximum length: 35	Fortinet_SSL_ECDSA256
certname-ecdsa384	384 bit ECDSA key certificate for re-signing server certificates for SSL inspection.	string	Maximum length: 35	Fortinet_SSL_ECDSA384
certname-ecdsa521	521 bit ECDSA key certificate for re-signing server certificates for SSL inspection.	string	Maximum length: 35	Fortinet_SSL_ECDSA521

Parameter	Description	Type	Size	Default						
certname-ed25519	253 bit EdDSA key certificate for re-signing server certificates for SSL inspection.	string	Maximum length: 35	Fortinet_SSL_ED25519						
certname-ed448	456 bit EdDSA key certificate for re-signing server certificates for SSL inspection.	string	Maximum length: 35	Fortinet_SSL_ED448						
certname-rsa1024	1024 bit RSA key certificate for re-signing server certificates for SSL inspection.	string	Maximum length: 35	Fortinet_SSL_RSA1024						
certname-rsa2048	2048 bit RSA key certificate for re-signing server certificates for SSL inspection.	string	Maximum length: 35	Fortinet_SSL_RSA2048						
certname-rsa4096	4096 bit RSA key certificate for re-signing server certificates for SSL inspection.	string	Maximum length: 35	Fortinet_SSL_RSA4096						
check-ca-cert	Enable/disable verification of the user certificate and pass authentication if any CA in the chain is trusted.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable verification of the user certificate.</td></tr><tr><td><i>disable</i></td><td>Disable verification of the user certificate.</td></tr></table>				Option	Description	<i>enable</i>	Enable verification of the user certificate.	<i>disable</i>	Disable verification of the user certificate.
Option	Description									
<i>enable</i>	Enable verification of the user certificate.									
<i>disable</i>	Disable verification of the user certificate.									
check-ca-chain	Enable/disable verification of the entire certificate chain and pass authentication only if the chain is complete and all of the CAs in the chain are trusted.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable verification of the entire certificate chain.</td></tr><tr><td><i>disable</i></td><td>Disable verification of the entire certificate chain.</td></tr></table>				Option	Description	<i>enable</i>	Enable verification of the entire certificate chain.	<i>disable</i>	Disable verification of the entire certificate chain.
Option	Description									
<i>enable</i>	Enable verification of the entire certificate chain.									
<i>disable</i>	Disable verification of the entire certificate chain.									
cmp-key-usage-checking	Enable/disable server certificate key usage checking in CMP mode.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable server certificate key usage checking in CMP mode.</td></tr><tr><td><i>disable</i></td><td>Disable server certificate key usage checking in CMP mode.</td></tr></table>				Option	Description	<i>enable</i>	Enable server certificate key usage checking in CMP mode.	<i>disable</i>	Disable server certificate key usage checking in CMP mode.
Option	Description									
<i>enable</i>	Enable server certificate key usage checking in CMP mode.									
<i>disable</i>	Disable server certificate key usage checking in CMP mode.									
cmp-save-extra-certs	Enable/disable saving extra certificates in CMP mode.	option	-	disable						

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable saving extra certificates in CMP mode.		
	<i>disable</i>	Disable saving extra certificates in CMP mode.		
cn-allow-multi	When searching for a matching certificate, allow multiple CN fields in certificate subject name.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Does not allow multiple CN entries in certificate matching.		
	<i>enable</i>	Allow multiple CN entries in certificate matching.		
cn-match	When searching for a matching certificate, control how to do CN value matching with certificate subject name.	option	-	substring
	<b>Option</b>	<b>Description</b>		
	<i>substring</i>	Find a match if the name being searched for is a part or the same as a certificate CN.		
	<i>value</i>	Find a match if the name being searched for is same as a certificate CN.		
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto
	<b>Option</b>	<b>Description</b>		
	<i>auto</i>	Set outgoing interface automatically.		
	<i>sdwan</i>	Set outgoing interface by SD-WAN or policy routing rules.		
	<i>specify</i>	Set outgoing interface manually.		
ocsp-default-server	Default OCSP server.	string	Maximum length: 35	
ocsp-option	Specify whether the OCSP URL is from certificate or configured OCSP server.	option	-	server
	<b>Option</b>	<b>Description</b>		
	<i>certificate</i>	Use URL from certificate.		
	<i>server</i>	Use URL from configured OCSP server.		
ocsp-status	Enable/disable receiving certificates using the OCSP.	option	-	disable

Parameter	Description	Type	Size	Default												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.									
Option	Description															
<i>enable</i>	Enable setting.															
<i>disable</i>	Disable setting.															
ssl-min-protocol-version	Minimum supported protocol version for SSL/TLS connections.	option	-	default												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>Follow system global setting.</td></tr><tr><td><i>SSLv3</i></td><td>SSLv3.</td></tr><tr><td><i>TLSv1</i></td><td>TLSv1.</td></tr><tr><td><i>TLSv1-1</i></td><td>TLSv1.1.</td></tr><tr><td><i>TLSv1-2</i></td><td>TLSv1.2.</td></tr></table>	Option	Description	<i>default</i>	Follow system global setting.	<i>SSLv3</i>	SSLv3.	<i>TLSv1</i>	TLSv1.	<i>TLSv1-1</i>	TLSv1.1.	<i>TLSv1-2</i>	TLSv1.2.			
Option	Description															
<i>default</i>	Follow system global setting.															
<i>SSLv3</i>	SSLv3.															
<i>TLSv1</i>	TLSv1.															
<i>TLSv1-1</i>	TLSv1.1.															
<i>TLSv1-2</i>	TLSv1.2.															
ssl-ocsp-source-ip	Source IP address to use to communicate with the OCSP server.	ipv4-address	Not Specified	0.0.0.0												
strict-ocsp-check	Enable/disable strict mode OCSP checking.	option	-	disable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable strict mode OCSP checking.</td></tr><tr><td><i>disable</i></td><td>Disable strict mode OCSP checking.</td></tr></table>	Option	Description	<i>enable</i>	Enable strict mode OCSP checking.	<i>disable</i>	Disable strict mode OCSP checking.									
Option	Description															
<i>enable</i>	Enable strict mode OCSP checking.															
<i>disable</i>	Disable strict mode OCSP checking.															
subject-match	When searching for a matching certificate, control how to do RDN value matching with certificate subject name.	option	-	substring												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>substring</i></td><td>Find a match if the name being searched for is a part or the same as a certificate subject RDN.</td></tr><tr><td><i>value</i></td><td>Find a match if the name being searched for is same as a certificate subject RDN.</td></tr></table>	Option	Description	<i>substring</i>	Find a match if the name being searched for is a part or the same as a certificate subject RDN.	<i>value</i>	Find a match if the name being searched for is same as a certificate subject RDN.									
Option	Description															
<i>substring</i>	Find a match if the name being searched for is a part or the same as a certificate subject RDN.															
<i>value</i>	Find a match if the name being searched for is same as a certificate subject RDN.															
subject-set	When searching for a matching certificate, control how to do RDN set matching with certificate subject name.	option	-	subset												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>subset</i></td><td>Find a match if the name being searched for is a subset of a certificate subject.</td></tr><tr><td><i>superset</i></td><td>Find a match if the name being searched for is a superset of a certificate subject.</td></tr></table>	Option	Description	<i>subset</i>	Find a match if the name being searched for is a subset of a certificate subject.	<i>superset</i>	Find a match if the name being searched for is a superset of a certificate subject.									
Option	Description															
<i>subset</i>	Find a match if the name being searched for is a subset of a certificate subject.															
<i>superset</i>	Find a match if the name being searched for is a superset of a certificate subject.															

## config crl-verification

Parameter	Description	Type	Size	Default						
expiry	CRL verification option when CRL is expired.	option	-	ignore						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ignore</td><td>Certificate status will be verified even if CRL is expired.</td></tr><tr><td>revoke</td><td>Certificate will be revoked if CRL is expired.</td></tr></table>	Option	Description	ignore	Certificate status will be verified even if CRL is expired.	revoke	Certificate will be revoked if CRL is expired.			
Option	Description									
ignore	Certificate status will be verified even if CRL is expired.									
revoke	Certificate will be revoked if CRL is expired.									
leaf-crl-absence	CRL verification option when leaf CRL is absent.	option	-	ignore						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ignore</td><td>CRL verification against leaf certificate is ignored if CRL is absent.</td></tr><tr><td>revoke</td><td>Certificate will be revoked if CRL of leaf certificate is absent.</td></tr></table>	Option	Description	ignore	CRL verification against leaf certificate is ignored if CRL is absent.	revoke	Certificate will be revoked if CRL of leaf certificate is absent.			
Option	Description									
ignore	CRL verification against leaf certificate is ignored if CRL is absent.									
revoke	Certificate will be revoked if CRL of leaf certificate is absent.									
chain-crl-absence	CRL verification option when CRL of any certificate in chain is absent.	option	-	ignore						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ignore</td><td>CRL verification is ignored if CRL of any certificate in chain is absent.</td></tr><tr><td>revoke</td><td>Certificate will be revoked if CRL of any certificate in chain is absent.</td></tr></table>	Option	Description	ignore	CRL verification is ignored if CRL of any certificate in chain is absent.	revoke	Certificate will be revoked if CRL of any certificate in chain is absent.			
Option	Description									
ignore	CRL verification is ignored if CRL of any certificate in chain is absent.									
revoke	Certificate will be revoked if CRL of any certificate in chain is absent.									

## config vpn ipsec concentrator

Concentrator configuration.

```
config vpn ipsec concentrator
  Description: Concentrator configuration.
  edit <id>
    set member <name1>, <name2>, ...
    set name {string}
    set src-check [disable|enable]
  next
end
```

## config vpn ipsec concentrator

Parameter	Description	Type	Size	Default
id	Concentrator ID.	integer	Minimum value: 1 Maximum value: 65535	0
member <name>	Names of up to 3 VPN tunnels to add to the concentrator. Member name.	string	Maximum length: 79	
name	Concentrator name.	string	Maximum length: 35	
src-check	Enable to check source address of phase 2 selector. Disable to check only the destination selector.	option	-	disable
		Option	Description	
		disable	Ignore source selector when choosing tunnel.	
		enable	Use source selector to choose tunnel.	

## config vpn ipsec fec

Configure Forward Error Correction (FEC) mapping profiles.

```
config vpn ipsec fec
  Description: Configure Forward Error Correction (FEC) mapping profiles.
  edit <name>
    config mappings
      Description: FEC redundancy mapping table.
      edit <seqno>
        set base {integer}
        set redundant {integer}
        set packet-loss-threshold {integer}
        set latency-threshold {integer}
        set bandwidth-up-threshold {integer}
        set bandwidth-down-threshold {integer}
        set bandwidth-bi-threshold {integer}
      next
    end
  next
end
```

## config vpn ipsec fec

Parameter	Description	Type	Size	Default
name	Profile name.	string	Maximum length: 35	

## config mappings

Parameter	Description	Type	Size	Default
seqno	Sequence number.	integer	Minimum value: 0 Maximum value: 64	0
base	Number of base FEC packets.	integer	Minimum value: 1 Maximum value: 20	0
redundant	Number of redundant FEC packets.	integer	Minimum value: 1 Maximum value: 5	0
packet-loss-threshold	Apply FEC parameters when packet loss is >= threshold.	integer	Minimum value: 0 Maximum value: 100	0
latency-threshold	Apply FEC parameters when latency is <= threshold (0 means no threshold).	integer	Minimum value: 0 Maximum value: 4294967295	0
bandwidth-up-threshold	Apply FEC parameters when available up bandwidth is >= threshold (kbps, 0 means no threshold).	integer	Minimum value: 0 Maximum value: 4294967295	0
bandwidth-down-threshold	Apply FEC parameters when available down bandwidth is >= threshold (kbps, 0 means no threshold).	integer	Minimum value: 0 Maximum value: 4294967295	0

Parameter	Description	Type	Size	Default
bandwidth-bi-threshold	Apply FEC parameters when available bi-bandwidth is >= threshold (kbps, 0 means no threshold).	integer	Minimum value: 0 Maximum value: 4294967295	0

## config vpn ipsec forticlient

Configure FortiClient policy realm.

```
config vpn ipsec forticlient
    Description: Configure FortiClient policy realm.
    edit <realm>
        set phase2name {string}
        set status [enable|disable]
        set usergroupname {string}
    next
end
```

## config vpn ipsec forticlient

Parameter	Description	Type	Size	Default						
phase2name	Phase 2 tunnel name that you defined in the FortiClient dialup configuration.	string	Maximum length: 35							
realm	FortiClient realm name.	string	Maximum length: 35							
status	Enable/disable this FortiClient configuration.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>				Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.
	Option	Description								
	<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.									
usergroupname	User group name for FortiClient users.	string	Maximum length: 35							

## config vpn ipsec manualkey-interface

Configure IPsec manual keys.

```
config vpn ipsec manualkey-interface
    Description: Configure IPsec manual keys.
    edit <name>
        set addr-type [4|6]
        set auth-alg [null|md5|...]
    next
end
```



```

    set auth-key {user}
    set enc-alg [null|des|...]
    set enc-key {user}
    set interface {string}
    set ip-version [4|6]
    set local-gw {ipv4-address-any}
    set local-gw6 {ipv6-address}
    set local-spi {user}
    set npu-offload [enable|disable]
    set remote-gw {ipv4-address}
    set remote-gw6 {ipv6-address}
    set remote-spi {user}
next
end

```

## config vpn ipsec manualkey-interface

Parameter	Description	Type	Size	Default														
addr-type	IP version to use for IP packets.	option	-	4														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>4</td><td>Use IPv4 addressing for IP packets.</td></tr><tr><td>6</td><td>Use IPv6 addressing for IP packets.</td></tr></table>	Option	Description	4	Use IPv4 addressing for IP packets.	6	Use IPv6 addressing for IP packets.											
Option	Description																	
4	Use IPv4 addressing for IP packets.																	
6	Use IPv6 addressing for IP packets.																	
auth-alg	Authentication algorithm. Must be the same for both ends of the tunnel.	option	-	null														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>null</td><td>null</td></tr><tr><td>md5</td><td>md5</td></tr><tr><td>sha1</td><td>sha1</td></tr><tr><td>sha256</td><td>sha256</td></tr><tr><td>sha384</td><td>sha384</td></tr><tr><td>sha512</td><td>sha512</td></tr></table>	Option	Description	null	null	md5	md5	sha1	sha1	sha256	sha256	sha384	sha384	sha512	sha512			
Option	Description																	
null	null																	
md5	md5																	
sha1	sha1																	
sha256	sha256																	
sha384	sha384																	
sha512	sha512																	
auth-key	Hexadecimal authentication key in 16-digit (8-byte) segments separated by hyphens.	user	Not Specified															
enc-alg	Encryption algorithm. Must be the same for both ends of the tunnel.	option	-	null														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>null</td><td>null</td></tr><tr><td>des</td><td>des</td></tr></table>	Option	Description	null	null	des	des											
Option	Description																	
null	null																	
des	des																	

Parameter	Description	Type	Size	Default																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>3des</td><td>3des</td></tr><tr><td>aes128</td><td>aes128</td></tr><tr><td>aes192</td><td>aes192</td></tr><tr><td>aes256</td><td>aes256</td></tr><tr><td>aria128</td><td>aria128</td></tr><tr><td>aria192</td><td>aria192</td></tr><tr><td>aria256</td><td>aria256</td></tr><tr><td>seed</td><td>seed</td></tr></table>	Option	Description	3des	3des	aes128	aes128	aes192	aes192	aes256	aes256	aria128	aria128	aria192	aria192	aria256	aria256	seed	seed			
	Option	Description																				
	3des	3des																				
	aes128	aes128																				
	aes192	aes192																				
	aes256	aes256																				
	aria128	aria128																				
	aria192	aria192																				
	aria256	aria256																				
seed	seed																					
enc-key	Hexadecimal encryption key in 16-digit (8-byte) segments separated by hyphens.	user	Not Specified																			
interface	Name of the physical, aggregate, or VLAN interface.	string	Maximum length: 15																			
ip-version	IP version to use for VPN interface.	option	-	4																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>4</td><td>Use IPv4 addressing for gateways.</td></tr><tr><td>6</td><td>Use IPv6 addressing for gateways.</td></tr></table>	Option	Description	4	Use IPv4 addressing for gateways.	6	Use IPv6 addressing for gateways.															
	Option	Description																				
	4	Use IPv4 addressing for gateways.																				
6	Use IPv6 addressing for gateways.																					
local-gw	IPv4 address of the local gateway's external interface.	ipv4-address-any	Not Specified	0.0.0.0																		
local-gw6	Local IPv6 address of VPN gateway.	ipv6-address	Not Specified	::																		
local-spi	Local SPI, a hexadecimal 8-digit (4-byte) tag. Discerns between two traffic streams with different encryption rules.	user	Not Specified																			
name	IPsec tunnel name.	string	Maximum length: 15																			
npu-offload *	Enable/disable offloading IPsec VPN manual key sessions to NPUs.	option	-	enable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable NPU offloading.</td></tr><tr><td>disable</td><td>Disable NPU offloading.</td></tr></table>	Option	Description	enable	Enable NPU offloading.	disable	Disable NPU offloading.															
	Option	Description																				
	enable	Enable NPU offloading.																				
disable	Disable NPU offloading.																					

Parameter	Description	Type	Size	Default
remote-gw	IPv4 address of the remote gateway's external interface.	ipv4-address	Not Specified	0.0.0.0
remote-gw6	Remote IPv6 address of VPN gateway.	ipv6-address	Not Specified	::
remote-spi	Remote SPI, a hexadecimal 8-digit (4-byte) tag. Discerns between two traffic streams with different encryption rules.	user	Not Specified	

\* This parameter may not exist in some models.

## config vpn ipsec manualkey

Configure IPsec manual keys.

```

config vpn ipsec manualkey
    Description: Configure IPsec manual keys.
    edit <name>
        set authentication [null|md5|...]
        set authkey {user}
        set enckey {user}
        set encryption [null|des|...]
        set interface {string}
        set local-gw {ipv4-address-any}
        set localspi {user}
        set npu-offload [enable|disable]
        set remote-gw {ipv4-address}
        set remotespi {user}
    next
end

```

## config vpn ipsec manualkey

Parameter	Description	Type	Size	Default
authentication	Authentication algorithm. Must be the same for both ends of the tunnel.	option	-	null
		Option	Description	
		<i>null</i>	Null.	
		<i>md5</i>	MD5.	
		<i>sha1</i>	SHA1.	
		<i>sha256</i>	SHA256.	
		<i>sha384</i>	SHA384.	
		<i>sha512</i>	SHA512.	

Parameter	Description	Type	Size	Default																						
authkey	Hexadecimal authentication key in 16-digit (8-byte) segments separated by hyphens.	user	Not Specified																							
enckey	Hexadecimal encryption key in 16-digit (8-byte) segments separated by hyphens.	user	Not Specified																							
encryption	Encryption algorithm. Must be the same for both ends of the tunnel.	option	-	null																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>null</i></td><td>Null.</td></tr><tr><td><i>des</i></td><td>DES.</td></tr><tr><td><i>3des</i></td><td>3DES.</td></tr><tr><td><i>aes128</i></td><td>AES128.</td></tr><tr><td><i>aes192</i></td><td>AES192.</td></tr><tr><td><i>aes256</i></td><td>AES256.</td></tr><tr><td><i>aria128</i></td><td>ARIA128.</td></tr><tr><td><i>aria192</i></td><td>ARIA192.</td></tr><tr><td><i>aria256</i></td><td>ARIA256.</td></tr><tr><td><i>seed</i></td><td>Seed.</td></tr></table>	Option	Description	<i>null</i>	Null.	<i>des</i>	DES.	<i>3des</i>	3DES.	<i>aes128</i>	AES128.	<i>aes192</i>	AES192.	<i>aes256</i>	AES256.	<i>aria128</i>	ARIA128.	<i>aria192</i>	ARIA192.	<i>aria256</i>	ARIA256.	<i>seed</i>	Seed.			
	Option	Description																								
	<i>null</i>	Null.																								
	<i>des</i>	DES.																								
	<i>3des</i>	3DES.																								
	<i>aes128</i>	AES128.																								
	<i>aes192</i>	AES192.																								
	<i>aes256</i>	AES256.																								
	<i>aria128</i>	ARIA128.																								
	<i>aria192</i>	ARIA192.																								
	<i>aria256</i>	ARIA256.																								
<i>seed</i>	Seed.																									
interface	Name of the physical, aggregate, or VLAN interface.	string	Maximum length: 15																							
local-gw	Local gateway.	ipv4-address-any	Not Specified	0.0.0.0																						
localspi	Local SPI, a hexadecimal 8-digit (4-byte) tag. Discerns between two traffic streams with different encryption rules.	user	Not Specified																							
name	IPsec tunnel name.	string	Maximum length: 35																							
npu-offload *	Enable/disable NPU offloading.	option	-	enable																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable NPU offloading.</td></tr><tr><td><i>disable</i></td><td>Disable NPU offloading.</td></tr></table>	Option	Description	<i>enable</i>	Enable NPU offloading.	<i>disable</i>	Disable NPU offloading.																			
	Option	Description																								
	<i>enable</i>	Enable NPU offloading.																								
<i>disable</i>	Disable NPU offloading.																									
remote-gw	Peer gateway.	ipv4-address	Not Specified	0.0.0.0																						

Parameter	Description	Type	Size	Default
remotespi	Remote SPI, a hexadecimal 8-digit (4-byte) tag. Discerns between two traffic streams with different encryption rules.	user	Not Specified	

\* This parameter may not exist in some models.

## config vpn ipsec phase1-interface

Configure VPN remote gateway.

```
config vpn ipsec phase1-interface
  Description: Configure VPN remote gateway.
  edit <name>
    set acct-verify [enable|disable]
    set add-gw-route [enable|disable]
    set add-route [disable|enable]
    set aggregate-member [enable|disable]
    set aggregate-weight {integer}
    set assign-ip [disable|enable]
    set assign-ip-from [range|usrgrp|...]
    set authmethod [psk|signature]
    set authmethod-remote [psk|signature]
    set authpasswd {password}
    set authusr {string}
    set authusrgrp {string}
    set auto-discovery-forwarder [enable|disable]
    set auto-discovery-psk [enable|disable]
    set auto-discovery-receiver [enable|disable]
    set auto-discovery-sender [enable|disable]
    set auto-discovery-shortcuts [independent|dependent]
    set auto-negotiate [enable|disable]
    set backup-gateway <address1>, <address2>, ...
    set banner {var-string}
    set cert-id-validation [enable|disable]
    set certificate <name1>, <name2>, ...
    set childless-ike [enable|disable]
    set client-auto-negotiate [disable|enable]
    set client-keep-alive [disable|enable]
    set comments {var-string}
    set default-gw {ipv4-address}
    set default-gw-priority {integer}
    set dhcp-ra-giaddr {ipv4-address}
    set dhcp6-ra-linkaddr {ipv6-address}
    set dhgrp {option1}, {option2}, ...
    set digital-signature-auth [enable|disable]
    set distance {integer}
    set dns-mode [manual|auto]
    set domain {string}
    set dpd [disable|on-idle|...]
    set dpd-retrycount {integer}
    set dpd-retryinterval {user}
    set eap [enable|disable]
```

```

set eap-exclude-peergrp {string}
set eap-identity [use-id-payload|send-request]
set encap-local-gw4 {ipv4-address}
set encap-local-gw6 {ipv6-address}
set encap-remote-gw4 {ipv4-address}
set encap-remote-gw6 {ipv6-address}
set encapsulation [none|gre|...]
set encapsulation-address [ike|ipv4|...]
set enforce-unique-id [disable|keep-new|...]
set esn [require|allow|...]
set exchange-interface-ip [enable|disable]
set exchange-ip-addr4 {ipv4-address}
set exchange-ip-addr6 {ipv6-address}
set fec-base {integer}
set fec-codec [rs|xor]
set fec-egress [enable|disable]
set fec-health-check {string}
set fec-ingress [enable|disable]
set fec-mapping-profile {string}
set fec-receive-timeout {integer}
set fec-redundant {integer}
set fec-send-timeout {integer}
set fgsp-sync [enable|disable]
set forticlient-enforcement [enable|disable]
set fragmentation [enable|disable]
set fragmentation-mtu {integer}
set group-authentication [enable|disable]
set group-authentication-secret {password-3}
set ha-sync-esp-seqno [enable|disable]
set idle-timeout [enable|disable]
set idle-timeoutinterval {integer}
set ike-version [1|2]
set inbound-dscp-copy [enable|disable]
set include-local-lan [disable|enable]
set interface {string}
set ip-delay-interval {integer}
set ip-fragmentation [pre-encapsulation|post-encapsulation]
set ip-version [4|6]
set ipv4-dns-server1 {ipv4-address}
set ipv4-dns-server2 {ipv4-address}
set ipv4-dns-server3 {ipv4-address}
set ipv4-end-ip {ipv4-address}
config ipv4-exclude-range
    Description: Configuration Method IPv4 exclude ranges.
    edit <id>
        set start-ip {ipv4-address}
        set end-ip {ipv4-address}
    next
end
set ipv4-name {string}
set ipv4-netmask {ipv4-netmask}
set ipv4-split-exclude {string}
set ipv4-split-include {string}
set ipv4-start-ip {ipv4-address}
set ipv4-wins-server1 {ipv4-address}
set ipv4-wins-server2 {ipv4-address}

```

```

set ipv6-dns-server1 {ipv6-address}
set ipv6-dns-server2 {ipv6-address}
set ipv6-dns-server3 {ipv6-address}
set ipv6-end-ip {ipv6-address}
config ipv6-exclude-range
    Description: Configuration method IPv6 exclude ranges.
    edit <id>
        set start-ip {ipv6-address}
        set end-ip {ipv6-address}
    next
end
set ipv6-name {string}
set ipv6-prefix {integer}
set ipv6-split-exclude {string}
set ipv6-split-include {string}
set ipv6-start-ip {ipv6-address}
set keepalive {integer}
set keylife {integer}
set local-gw {ipv4-address}
set local-gw6 {ipv6-address}
set localid {string}
set localid-type [auto|fqdn|...]
set loopback-asymroute [enable|disable]
set mesh-selector-type [disable|subnet|...]
set mode [aggressive|main]
set mode-cfg [disable|enable]
set monitor {string}
set monitor-hold-down-delay {integer}
set monitor-hold-down-time {user}
set monitor-hold-down-type [immediate|delay|...]
set monitor-hold-down-weekday [everyday|sunday|...]
set nattraversal [enable|disable|...]
set negotiate-timeout {integer}
set net-device [enable|disable]
set network-id {integer}
set network-overlay [disable|enable]
set npu-offload [enable|disable]
set passive-mode [enable|disable]
set peer {string}
set peergrp {string}
set peerid {string}
set peertype [any|one|...]
set ppk [disable|allow|...]
set ppk-identity {string}
set ppk-secret {password-3}
set priority {integer}
set proposal {option1}, {option2}, ...
set psksecret {password-3}
set psksecret-remote {password-3}
set reauth [disable|enable]
set rekey [enable|disable]
set remote-gw {ipv4-address}
set remote-gw6 {ipv6-address}
set remotegw-ddns {string}
set rsa-signature-format [pkcs1|pss]
set save-password [disable|enable]

```

```

set send-cert-chain [enable|disable]
set signature-hash-alg {option1}, {option2}, ...
set split-include-service {string}
set suite-b [disable|suite-b-gcm-128|...]
set type [static|dynamic|...]
set unity-support [disable|enable]
set usrgrp {string}
set vni {integer}
set wizard-type [custom|dialup-forticlient|...]
set xauthtype [disable|client|...]
next
end

```

## config vpn ipsec phase1-interface

Parameter	Description	Type	Size	Default						
acct-verify	Enable/disable verification of RADIUS accounting record.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable verification of RADIUS accounting record.</td></tr><tr><td><i>disable</i></td><td>Disable verification of RADIUS accounting record.</td></tr></table>	Option	Description	<i>enable</i>	Enable verification of RADIUS accounting record.	<i>disable</i>	Disable verification of RADIUS accounting record.			
Option	Description									
<i>enable</i>	Enable verification of RADIUS accounting record.									
<i>disable</i>	Disable verification of RADIUS accounting record.									
add-gw-route	Enable/disable automatically add a route to the remote gateway.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Automatically add a route to the remote gateway.</td></tr><tr><td><i>disable</i></td><td>Do not automatically add a route to the remote gateway.</td></tr></table>	Option	Description	<i>enable</i>	Automatically add a route to the remote gateway.	<i>disable</i>	Do not automatically add a route to the remote gateway.			
Option	Description									
<i>enable</i>	Automatically add a route to the remote gateway.									
<i>disable</i>	Do not automatically add a route to the remote gateway.									
add-route	Enable/disable control addition of a route to peer destination selector.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Do not add a route to destination of peer selector.</td></tr><tr><td><i>enable</i></td><td>Add route to destination of peer selector.</td></tr></table>	Option	Description	<i>disable</i>	Do not add a route to destination of peer selector.	<i>enable</i>	Add route to destination of peer selector.			
Option	Description									
<i>disable</i>	Do not add a route to destination of peer selector.									
<i>enable</i>	Add route to destination of peer selector.									
aggregate-member	Enable/disable use as an aggregate member.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable use as an aggregate member.</td></tr><tr><td><i>disable</i></td><td>Disable use as an aggregate member.</td></tr></table>	Option	Description	<i>enable</i>	Enable use as an aggregate member.	<i>disable</i>	Disable use as an aggregate member.			
Option	Description									
<i>enable</i>	Enable use as an aggregate member.									
<i>disable</i>	Disable use as an aggregate member.									



Parameter	Description	Type	Size	Default										
aggregate-weight	Link weight for aggregate.	integer	Minimum value: 1 Maximum value: 100	1										
assign-ip	Enable/disable assignment of IP to IPsec interface via configuration method.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Do not assign an IP address to the IPsec interface.</td></tr><tr><td><i>enable</i></td><td>Assign an IP address to the IPsec interface.</td></tr></table>	Option	Description	<i>disable</i>	Do not assign an IP address to the IPsec interface.	<i>enable</i>	Assign an IP address to the IPsec interface.							
Option	Description													
<i>disable</i>	Do not assign an IP address to the IPsec interface.													
<i>enable</i>	Assign an IP address to the IPsec interface.													
assign-ip-from	Method by which the IP address will be assigned.	option	-	range										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>range</i></td><td>Assign IP address from locally defined range.</td></tr><tr><td><i>usrgrp</i></td><td>Assign IP address via user group.</td></tr><tr><td><i>dhcp</i></td><td>Assign IP address via DHCP.</td></tr><tr><td><i>name</i></td><td>Assign IP address from firewall address or group.</td></tr></table>	Option	Description	<i>range</i>	Assign IP address from locally defined range.	<i>usrgrp</i>	Assign IP address via user group.	<i>dhcp</i>	Assign IP address via DHCP.	<i>name</i>	Assign IP address from firewall address or group.			
Option	Description													
<i>range</i>	Assign IP address from locally defined range.													
<i>usrgrp</i>	Assign IP address via user group.													
<i>dhcp</i>	Assign IP address via DHCP.													
<i>name</i>	Assign IP address from firewall address or group.													
authmethod	Authentication method.	option	-	psk										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>psk</i></td><td>PSK authentication method.</td></tr><tr><td><i>signature</i></td><td>Signature authentication method.</td></tr></table>	Option	Description	<i>psk</i>	PSK authentication method.	<i>signature</i>	Signature authentication method.							
Option	Description													
<i>psk</i>	PSK authentication method.													
<i>signature</i>	Signature authentication method.													
authmethod-remote	Authentication method (remote side).	option	-											
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>psk</i></td><td>PSK authentication method.</td></tr><tr><td><i>signature</i></td><td>Signature authentication method.</td></tr></table>	Option	Description	<i>psk</i>	PSK authentication method.	<i>signature</i>	Signature authentication method.							
Option	Description													
<i>psk</i>	PSK authentication method.													
<i>signature</i>	Signature authentication method.													
authpasswd	XAuth password (max 35 characters).	password	Not Specified											
authusr	XAuth user name.	string	Maximum length: 64											
authusrgrp	Authentication user group.	string	Maximum length: 35											
auto-discovery-forwarder	Enable/disable forwarding auto-discovery short-cut messages.	option	-	disable										

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable forwarding auto-discovery short-cut messages.		
	<i>disable</i>	Disable forwarding auto-discovery short-cut messages.		
auto-discovery-psk	Enable/disable use of pre-shared secrets for authentication of auto-discovery tunnels.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable use of pre-shared-secret authentication for auto-discovery tunnels.		
	<i>disable</i>	Disable use of authentication defined by 'authmethod' for auto-discovery tunnels.		
auto-discovery-receiver	Enable/disable accepting auto-discovery short-cut messages.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable receiving auto-discovery short-cut messages.		
	<i>disable</i>	Disable receiving auto-discovery short-cut messages.		
auto-discovery-sender	Enable/disable sending auto-discovery short-cut messages.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable sending auto-discovery short-cut messages.		
	<i>disable</i>	Disable sending auto-discovery short-cut messages.		
auto-discovery-shortcuts	Control deletion of child short-cut tunnels when the parent tunnel goes down.	option	-	independent
	<b>Option</b>	<b>Description</b>		
	<i>independent</i>	Short-cut tunnels remain up if the parent tunnel goes down.		
	<i>dependent</i>	Short-cut tunnels are brought down if the parent tunnel goes down.		
auto-negotiate	Enable/disable automatic initiation of IKE SA negotiation.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable automatic initiation of IKE SA negotiation.		
	<i>disable</i>	Disable automatic initiation of IKE SA negotiation.		

Parameter	Description	Type	Size	Default						
backup-gateway <address>	Instruct unity clients about the backup gateway address(es). Address of backup gateway.	string	Maximum length: 79							
banner	Message that unity client should display after connecting.	var-string	Maximum length: 1024							
cert-id-validation	Enable/disable cross validation of peer ID and the identity in the peer's certificate as specified in RFC 4945.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable cross validation of peer ID and the identity in the peer's certificate as specified in RFC 4945.</td></tr><tr><td><i>disable</i></td><td>Disable cross validation of peer ID and the identity in the peer's certificate as specified in RFC 4945.</td></tr></table>				Option	Description	<i>enable</i>	Enable cross validation of peer ID and the identity in the peer's certificate as specified in RFC 4945.	<i>disable</i>	Disable cross validation of peer ID and the identity in the peer's certificate as specified in RFC 4945.
Option	Description									
<i>enable</i>	Enable cross validation of peer ID and the identity in the peer's certificate as specified in RFC 4945.									
<i>disable</i>	Disable cross validation of peer ID and the identity in the peer's certificate as specified in RFC 4945.									
certificate <name>	The names of up to 4 signed personal certificates. Certificate name.	string	Maximum length: 79							
childless-ike	Enable/disable childless IKEv2 initiation (RFC 6023).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable childless IKEv2 initiation (RFC 6023).</td></tr><tr><td><i>disable</i></td><td>Disable childless IKEv2 initiation (RFC 6023).</td></tr></table>				Option	Description	<i>enable</i>	Enable childless IKEv2 initiation (RFC 6023).	<i>disable</i>	Disable childless IKEv2 initiation (RFC 6023).
Option	Description									
<i>enable</i>	Enable childless IKEv2 initiation (RFC 6023).									
<i>disable</i>	Disable childless IKEv2 initiation (RFC 6023).									
client-auto-negotiate	Enable/disable allowing the VPN client to bring up the tunnel when there is no traffic.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable allowing the VPN client to bring up the tunnel when there is no traffic.</td></tr><tr><td><i>enable</i></td><td>Enable allowing the VPN client to bring up the tunnel when there is no traffic.</td></tr></table>				Option	Description	<i>disable</i>	Disable allowing the VPN client to bring up the tunnel when there is no traffic.	<i>enable</i>	Enable allowing the VPN client to bring up the tunnel when there is no traffic.
Option	Description									
<i>disable</i>	Disable allowing the VPN client to bring up the tunnel when there is no traffic.									
<i>enable</i>	Enable allowing the VPN client to bring up the tunnel when there is no traffic.									
client-keep-alive	Enable/disable allowing the VPN client to keep the tunnel up when there is no traffic.	option	-	disable						

Parameter	Description	Type	Size	Default																												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable allowing the VPN client to keep the tunnel up when there is no traffic.</td></tr><tr><td><i>enable</i></td><td>Enable allowing the VPN client to keep the tunnel up when there is no traffic.</td></tr></table>	Option	Description	<i>disable</i>	Disable allowing the VPN client to keep the tunnel up when there is no traffic.	<i>enable</i>	Enable allowing the VPN client to keep the tunnel up when there is no traffic.																									
	Option	Description																														
	<i>disable</i>	Disable allowing the VPN client to keep the tunnel up when there is no traffic.																														
<i>enable</i>	Enable allowing the VPN client to keep the tunnel up when there is no traffic.																															
comments	Comment.	var-string	Maximum length: 255																													
default-gw	IPv4 address of default route gateway to use for traffic exiting the interface.	ipv4-address	Not Specified	0.0.0.0																												
default-gw-priority	Priority for default gateway route. A higher priority number signifies a less preferred route.	integer	Minimum value: 0 Maximum value: 4294967295	0																												
dhcp-ra-giaddr	Relay agent gateway IP address to use in the giaddr field of DHCP requests.	ipv4-address	Not Specified	0.0.0.0																												
dhcp6-ra-linkaddr	Relay agent IPv6 link address to use in DHCP6 requests.	ipv6-address	Not Specified	::																												
dhgrp	DH group.	option	-	14																												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>1</td><td>DH Group 1.</td></tr><tr><td>2</td><td>DH Group 2.</td></tr><tr><td>5</td><td>DH Group 5.</td></tr><tr><td>14</td><td>DH Group 14.</td></tr><tr><td>15</td><td>DH Group 15.</td></tr><tr><td>16</td><td>DH Group 16.</td></tr><tr><td>17</td><td>DH Group 17.</td></tr><tr><td>18</td><td>DH Group 18.</td></tr><tr><td>19</td><td>DH Group 19.</td></tr><tr><td>20</td><td>DH Group 20.</td></tr><tr><td>21</td><td>DH Group 21.</td></tr><tr><td>27</td><td>DH Group 27.</td></tr><tr><td>28</td><td>DH Group 28.</td></tr></table>	Option	Description	1	DH Group 1.	2	DH Group 2.	5	DH Group 5.	14	DH Group 14.	15	DH Group 15.	16	DH Group 16.	17	DH Group 17.	18	DH Group 18.	19	DH Group 19.	20	DH Group 20.	21	DH Group 21.	27	DH Group 27.	28	DH Group 28.			
	Option	Description																														
	1	DH Group 1.																														
	2	DH Group 2.																														
	5	DH Group 5.																														
	14	DH Group 14.																														
	15	DH Group 15.																														
	16	DH Group 16.																														
	17	DH Group 17.																														
	18	DH Group 18.																														
	19	DH Group 19.																														
	20	DH Group 20.																														
	21	DH Group 21.																														
	27	DH Group 27.																														
	28	DH Group 28.																														

Parameter	Description	Type	Size	Default										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>29</td><td>DH Group 29.</td></tr><tr><td>30</td><td>DH Group 30.</td></tr><tr><td>31</td><td>DH Group 31.</td></tr><tr><td>32</td><td>DH Group 32.</td></tr></table>	Option	Description	29	DH Group 29.	30	DH Group 30.	31	DH Group 31.	32	DH Group 32.			
	Option	Description												
	29	DH Group 29.												
	30	DH Group 30.												
	31	DH Group 31.												
32	DH Group 32.													
digital-signature-auth	Enable/disable IKEv2 Digital Signature Authentication (RFC 7427).	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable IKEv2 Digital Signature Authentication (RFC 7427).</td></tr><tr><td>disable</td><td>Disable IKEv2 Digital Signature Authentication (RFC 7427).</td></tr></table>	Option	Description	enable	Enable IKEv2 Digital Signature Authentication (RFC 7427).	disable	Disable IKEv2 Digital Signature Authentication (RFC 7427).							
	Option	Description												
	enable	Enable IKEv2 Digital Signature Authentication (RFC 7427).												
disable	Disable IKEv2 Digital Signature Authentication (RFC 7427).													
distance	Distance for routes added by IKE.	integer	Minimum value: 1 Maximum value: 255	15										
dns-mode	DNS server mode.	option	-	manual										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>manual</td><td>Manually configure DNS servers.</td></tr><tr><td>auto</td><td>Use default DNS servers.</td></tr></table>	Option	Description	manual	Manually configure DNS servers.	auto	Use default DNS servers.							
	Option	Description												
	manual	Manually configure DNS servers.												
auto	Use default DNS servers.													
domain	Instruct unity clients about the single default DNS domain.	string	Maximum length: 63											
dpd	Dead Peer Detection mode.	option	-	on-demand										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable Dead Peer Detection.</td></tr><tr><td>on-idle</td><td>Trigger Dead Peer Detection when IPsec is idle.</td></tr><tr><td>on-demand</td><td>Trigger Dead Peer Detection when IPsec traffic is sent but no reply is received from the peer.</td></tr></table>	Option	Description	disable	Disable Dead Peer Detection.	on-idle	Trigger Dead Peer Detection when IPsec is idle.	on-demand	Trigger Dead Peer Detection when IPsec traffic is sent but no reply is received from the peer.					
	Option	Description												
	disable	Disable Dead Peer Detection.												
	on-idle	Trigger Dead Peer Detection when IPsec is idle.												
on-demand	Trigger Dead Peer Detection when IPsec traffic is sent but no reply is received from the peer.													
dpd-retrycount	Number of DPD retry attempts.	integer	Minimum value: 0 Maximum value: 10	3										
dpd-retryinterval	DPD retry interval.	user	Not Specified											

Parameter	Description	Type	Size	Default								
eap	Enable/disable IKEv2 EAP authentication.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable IKEv2 EAP authentication.</td></tr><tr><td><i>disable</i></td><td>Disable IKEv2 EAP authentication.</td></tr></table>	Option	Description	<i>enable</i>	Enable IKEv2 EAP authentication.	<i>disable</i>	Disable IKEv2 EAP authentication.					
Option	Description											
<i>enable</i>	Enable IKEv2 EAP authentication.											
<i>disable</i>	Disable IKEv2 EAP authentication.											
eap-exclude-peergrp	Peer group excluded from EAP authentication.	string	Maximum length: 35									
eap-identity	IKEv2 EAP peer identity type.	option	-	use-id-payload								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>use-id-payload</i></td><td>Use IKEv2 IDi payload to resolve peer identity.</td></tr><tr><td><i>send-request</i></td><td>Use EAP identity request to resolve peer identity.</td></tr></table>	Option	Description	<i>use-id-payload</i>	Use IKEv2 IDi payload to resolve peer identity.	<i>send-request</i>	Use EAP identity request to resolve peer identity.					
Option	Description											
<i>use-id-payload</i>	Use IKEv2 IDi payload to resolve peer identity.											
<i>send-request</i>	Use EAP identity request to resolve peer identity.											
encap-local-gw4	Local IPv4 address of GRE/VXLAN tunnel.	ipv4-address	Not Specified	0.0.0.0								
encap-local-gw6	Local IPv6 address of GRE/VXLAN tunnel.	ipv6-address	Not Specified	::								
encap-remote-gw4	Remote IPv4 address of GRE/VXLAN tunnel.	ipv4-address	Not Specified	0.0.0.0								
encap-remote-gw6	Remote IPv6 address of GRE/VXLAN tunnel.	ipv6-address	Not Specified	::								
encapsulation	Enable/disable GRE/VXLAN encapsulation.	option	-	none								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>No additional encapsulation.</td></tr><tr><td><i>gre</i></td><td>GRE encapsulation.</td></tr><tr><td><i>vxlan</i></td><td>VXLAN encapsulation.</td></tr></table>	Option	Description	<i>none</i>	No additional encapsulation.	<i>gre</i>	GRE encapsulation.	<i>vxlan</i>	VXLAN encapsulation.			
Option	Description											
<i>none</i>	No additional encapsulation.											
<i>gre</i>	GRE encapsulation.											
<i>vxlan</i>	VXLAN encapsulation.											
encapsulation-address	Source for GRE/VXLAN tunnel address.	option	-	ike								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ike</i></td><td>Use IKE/IPsec gateway addresses.</td></tr><tr><td><i>ipv4</i></td><td>Specify separate GRE/VXLAN tunnel address.</td></tr><tr><td><i>ipv6</i></td><td>Specify separate GRE/VXLAN tunnel address.</td></tr></table>	Option	Description	<i>ike</i>	Use IKE/IPsec gateway addresses.	<i>ipv4</i>	Specify separate GRE/VXLAN tunnel address.	<i>ipv6</i>	Specify separate GRE/VXLAN tunnel address.			
Option	Description											
<i>ike</i>	Use IKE/IPsec gateway addresses.											
<i>ipv4</i>	Specify separate GRE/VXLAN tunnel address.											
<i>ipv6</i>	Specify separate GRE/VXLAN tunnel address.											

Parameter	Description	Type	Size	Default								
enforce-unique-id	Enable/disable peer ID uniqueness check.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable peer ID uniqueness enforcement.</td></tr><tr><td>keep-new</td><td>Enforce peer ID uniqueness, keep new connection if collision found.</td></tr><tr><td>keep-old</td><td>Enforce peer ID uniqueness, keep old connection if collision found.</td></tr></table>	Option	Description	disable	Disable peer ID uniqueness enforcement.	keep-new	Enforce peer ID uniqueness, keep new connection if collision found.	keep-old	Enforce peer ID uniqueness, keep old connection if collision found.			
Option	Description											
disable	Disable peer ID uniqueness enforcement.											
keep-new	Enforce peer ID uniqueness, keep new connection if collision found.											
keep-old	Enforce peer ID uniqueness, keep old connection if collision found.											
esn *	Extended sequence number (ESN) negotiation.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>require</td><td>Require extended sequence number.</td></tr><tr><td>allow</td><td>Allow extended sequence number.</td></tr><tr><td>disable</td><td>Disable extended sequence number.</td></tr></table>	Option	Description	require	Require extended sequence number.	allow	Allow extended sequence number.	disable	Disable extended sequence number.			
Option	Description											
require	Require extended sequence number.											
allow	Allow extended sequence number.											
disable	Disable extended sequence number.											
exchange-interface-ip	Enable/disable exchange of IPsec interface IP address.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable exchange of IPsec interface IP address.</td></tr><tr><td>disable</td><td>Disable exchange of IPsec interface IP address.</td></tr></table>	Option	Description	enable	Enable exchange of IPsec interface IP address.	disable	Disable exchange of IPsec interface IP address.					
Option	Description											
enable	Enable exchange of IPsec interface IP address.											
disable	Disable exchange of IPsec interface IP address.											
exchange-ip-addr4	IPv4 address to exchange with peers.	ipv4-address	Not Specified	0.0.0.0								
exchange-ip-addr6	IPv6 address to exchange with peers.	ipv6-address	Not Specified	::								
fec-base	Number of base Forward Error Correction packets.	integer	Minimum value: 1 Maximum value: 20	10								
fec-codec	Forward Error Correction encoding/decoding algorithm.	option	-	rs								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>rs</td><td>Reed-Solomon FEC algorithm.</td></tr><tr><td>xor</td><td>XOR FEC algorithm.</td></tr></table>	Option	Description	rs	Reed-Solomon FEC algorithm.	xor	XOR FEC algorithm.					
Option	Description											
rs	Reed-Solomon FEC algorithm.											
xor	XOR FEC algorithm.											
fec-egress	Enable/disable Forward Error Correction for egress IPsec traffic.	option	-	disable								

Parameter	Description	Type	Size	Default
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Enable Forward Error Correction for egress IPsec traffic.		
	<i>disable</i>	Disable Forward Error Correction for egress IPsec traffic.		
fec-health-check	SD-WAN health check.	string	Maximum length: 35	
fec-ingress	Enable/disable Forward Error Correction for ingress IPsec traffic.	option	-	disable
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Enable Forward Error Correction for ingress IPsec traffic.		
	<i>disable</i>	Disable Forward Error Correction for ingress IPsec traffic.		
fec-mapping-profile	Forward Error Correction (FEC) mapping profile.	string	Maximum length: 35	
fec-receive-timeout	Timeout in milliseconds before dropping Forward Error Correction packets.	integer	Minimum value: 1 Maximum value: 1000	50
fec-redundant	Number of redundant Forward Error Correction packets.	integer	Minimum value: 1 Maximum value: 5	1
fec-send-timeout	Timeout in milliseconds before sending Forward Error Correction packets.	integer	Minimum value: 1 Maximum value: 1000	5
fgsp-sync	Enable/disable IPsec syncing of tunnels for FGSP IPsec.	option	-	disable
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Enable IPsec syncing of tunnels to other cluster members.		
	<i>disable</i>	Disable IPsec syncing of tunnels to other cluster members.		
forticlient-enforcement	Enable/disable FortiClient enforcement.	option	-	disable
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Enable FortiClient enforcement.		
	<i>disable</i>	Disable FortiClient enforcement.		



Parameter	Description	Type	Size	Default						
fragmentation	Enable/disable fragment IKE message on re-transmission.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable intra-IKE fragmentation support on re-transmission.</td></tr><tr><td><i>disable</i></td><td>Disable intra-IKE fragmentation support.</td></tr></table>				Option	Description	<i>enable</i>	Enable intra-IKE fragmentation support on re-transmission.	<i>disable</i>	Disable intra-IKE fragmentation support.
	Option	Description								
	<i>enable</i>	Enable intra-IKE fragmentation support on re-transmission.								
<i>disable</i>	Disable intra-IKE fragmentation support.									
fragmentation-mtu	IKE fragmentation MTU.	integer	Minimum value: 500 Maximum value: 16000	1200						
group-authentication	Enable/disable IKEv2 IDi group authentication.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable IKEv2 IDi group authentication.</td></tr><tr><td><i>disable</i></td><td>Disable IKEv2 IDi group authentication.</td></tr></table>				Option	Description	<i>enable</i>	Enable IKEv2 IDi group authentication.	<i>disable</i>	Disable IKEv2 IDi group authentication.
	Option	Description								
	<i>enable</i>	Enable IKEv2 IDi group authentication.								
<i>disable</i>	Disable IKEv2 IDi group authentication.									
group-authentication-secret	Password for IKEv2 ID group authentication. ASCII string or hexadecimal indicated by a leading 0x.	password-3	Not Specified							
ha-sync-esp-seqno	Enable/disable sequence number jump ahead for IPsec HA.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable HA syncing of ESP sequence numbers.</td></tr><tr><td><i>disable</i></td><td>Disable HA syncing of ESP sequence numbers.</td></tr></table>				Option	Description	<i>enable</i>	Enable HA syncing of ESP sequence numbers.	<i>disable</i>	Disable HA syncing of ESP sequence numbers.
	Option	Description								
	<i>enable</i>	Enable HA syncing of ESP sequence numbers.								
<i>disable</i>	Disable HA syncing of ESP sequence numbers.									
idle-timeout	Enable/disable IPsec tunnel idle timeout.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable IPsec tunnel idle timeout.</td></tr><tr><td><i>disable</i></td><td>Disable IPsec tunnel idle timeout.</td></tr></table>				Option	Description	<i>enable</i>	Enable IPsec tunnel idle timeout.	<i>disable</i>	Disable IPsec tunnel idle timeout.
	Option	Description								
	<i>enable</i>	Enable IPsec tunnel idle timeout.								
<i>disable</i>	Disable IPsec tunnel idle timeout.									
idle-timeoutinterval	IPsec tunnel idle timeout in minutes.	integer	Minimum value: 5 Maximum value: 43200	15						
ike-version	IKE protocol version.	option	-	1						

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>1</td><td>Use IKEv1 protocol.</td></tr><tr><td>2</td><td>Use IKEv2 protocol.</td></tr></table>	Option	Description	1	Use IKEv1 protocol.	2	Use IKEv2 protocol.			
	Option	Description								
	1	Use IKEv1 protocol.								
2	Use IKEv2 protocol.									
inbound-dscp-copy	Enable/disable copying of the DSCP values in the ESP header to the inner IP Header.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable copying of the DSCP values in the ESP header to the inner IP Header.</td></tr><tr><td>disable</td><td>Disable copying of the DSCP values in the ESP header to the inner IP Header.</td></tr></table>	Option	Description	enable	Enable copying of the DSCP values in the ESP header to the inner IP Header.	disable	Disable copying of the DSCP values in the ESP header to the inner IP Header.			
	Option	Description								
	enable	Enable copying of the DSCP values in the ESP header to the inner IP Header.								
disable	Disable copying of the DSCP values in the ESP header to the inner IP Header.									
include-local-lan	Enable/disable allow local LAN access on unity clients.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable local LAN access on Unity clients.</td></tr><tr><td>enable</td><td>Enable local LAN access on Unity clients.</td></tr></table>	Option	Description	disable	Disable local LAN access on Unity clients.	enable	Enable local LAN access on Unity clients.			
	Option	Description								
	disable	Disable local LAN access on Unity clients.								
enable	Enable local LAN access on Unity clients.									
interface	Local physical, aggregate, or VLAN outgoing interface.	string	Maximum length: 35							
ip-delay-interval	IP address reuse delay interval in seconds.	integer	Minimum value: 0 Maximum value: 28800	0						
ip-fragmentation	Determine whether IP packets are fragmented before or after IPsec encapsulation.	option	-	post-encapsulation						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>pre-encapsulation</td><td>Fragment before IPsec encapsulation.</td></tr><tr><td>post-encapsulation</td><td>Fragment after IPsec encapsulation (RFC compliant).</td></tr></table>	Option	Description	pre-encapsulation	Fragment before IPsec encapsulation.	post-encapsulation	Fragment after IPsec encapsulation (RFC compliant).			
	Option	Description								
	pre-encapsulation	Fragment before IPsec encapsulation.								
post-encapsulation	Fragment after IPsec encapsulation (RFC compliant).									
ip-version	IP version to use for VPN interface.	option	-	4						

Parameter	Description	Type	Size	Default
	Option	Description		
	4	Use IPv4 addressing for gateways.		
	6	Use IPv6 addressing for gateways.		
ipv4-dns-server1	IPv4 DNS server 1.	ipv4-address	Not Specified	0.0.0.0
ipv4-dns-server2	IPv4 DNS server 2.	ipv4-address	Not Specified	0.0.0.0
ipv4-dns-server3	IPv4 DNS server 3.	ipv4-address	Not Specified	0.0.0.0
ipv4-end-ip	End of IPv4 range.	ipv4-address	Not Specified	0.0.0.0
ipv4-name	IPv4 address name.	string	Maximum length: 79	
ipv4-netmask	IPv4 Netmask.	ipv4-netmask	Not Specified	255.255.255.255
ipv4-split-exclude	IPv4 subnets that should not be sent over the IPsec tunnel.	string	Maximum length: 79	
ipv4-split-include	IPv4 split-include subnets.	string	Maximum length: 79	
ipv4-start-ip	Start of IPv4 range.	ipv4-address	Not Specified	0.0.0.0
ipv4-wins-server1	WINS server 1.	ipv4-address	Not Specified	0.0.0.0
ipv4-wins-server2	WINS server 2.	ipv4-address	Not Specified	0.0.0.0
ipv6-dns-server1	IPv6 DNS server 1.	ipv6-address	Not Specified	::
ipv6-dns-server2	IPv6 DNS server 2.	ipv6-address	Not Specified	::
ipv6-dns-server3	IPv6 DNS server 3.	ipv6-address	Not Specified	::
ipv6-end-ip	End of IPv6 range.	ipv6-address	Not Specified	::
ipv6-name	IPv6 address name.	string	Maximum length: 79	
ipv6-prefix	IPv6 prefix.	integer	Minimum value: 1 Maximum value: 128	128
ipv6-split-exclude	IPv6 subnets that should not be sent over the IPsec tunnel.	string	Maximum length: 79	
ipv6-split-include	IPv6 split-include subnets.	string	Maximum length: 79	

Parameter	Description	Type	Size	Default														
ipv6-start-ip	Start of IPv6 range.	ipv6-address	Not Specified	::														
keepalive	NAT-T keep alive interval.	integer	Minimum value: 10 Maximum value: 900	10														
keylife	Time to wait in seconds before phase 1 encryption key expires.	integer	Minimum value: 120 Maximum value: 172800	86400														
local-gw	IPv4 address of the local gateway's external interface.	ipv4-address	Not Specified	0.0.0.0														
local-gw6	IPv6 address of the local gateway's external interface.	ipv6-address	Not Specified	::														
localid	Local ID.	string	Maximum length: 63															
localid-type	Local ID type.	option	-	auto														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>auto</td><td>Select ID type automatically.</td></tr><tr><td>fqdn</td><td>Use fully qualified domain name.</td></tr><tr><td>user-fqdn</td><td>Use user fully qualified domain name.</td></tr><tr><td>keyid</td><td>Use key-id string.</td></tr><tr><td>address</td><td>Use local IP address.</td></tr><tr><td>asn1dn</td><td>Use ASN.1 distinguished name.</td></tr></table>				Option	Description	auto	Select ID type automatically.	fqdn	Use fully qualified domain name.	user-fqdn	Use user fully qualified domain name.	keyid	Use key-id string.	address	Use local IP address.	asn1dn	Use ASN.1 distinguished name.
Option	Description																	
auto	Select ID type automatically.																	
fqdn	Use fully qualified domain name.																	
user-fqdn	Use user fully qualified domain name.																	
keyid	Use key-id string.																	
address	Use local IP address.																	
asn1dn	Use ASN.1 distinguished name.																	
loopback-asymroute	Enable/disable asymmetric routing for IKE traffic on loopback interface.	option	-	enable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Allow ingress/egress IKE traffic to be routed over different interfaces.</td></tr><tr><td>disable</td><td>Ingress/egress IKE traffic must be routed over the same interface.</td></tr></table>				Option	Description	enable	Allow ingress/egress IKE traffic to be routed over different interfaces.	disable	Ingress/egress IKE traffic must be routed over the same interface.								
Option	Description																	
enable	Allow ingress/egress IKE traffic to be routed over different interfaces.																	
disable	Ingress/egress IKE traffic must be routed over the same interface.																	
mesh-selector-type	Add selectors containing subsets of the configuration depending on traffic.	option	-	disable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable.</td></tr></table>				Option	Description	disable	Disable.										
Option	Description																	
disable	Disable.																	

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>subnet</i>	Enable addition of matching subnet selector.		
	<i>host</i>	Enable addition of host to host selector.		
mode	The ID protection mode used to establish a secure channel.	option	-	main
	<b>Option</b>	<b>Description</b>		
	<i>aggressive</i>	Aggressive mode.		
	<i>main</i>	Main mode.		
mode-cfg	Enable/disable configuration method.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable Configuration Method.		
	<i>enable</i>	Enable Configuration Method.		
monitor	IPsec interface as backup for primary interface.	string	Maximum length: 35	
monitor-hold-down-delay	Time to wait in seconds before recovery once primary re-establishes.	integer	Minimum value: 0 Maximum value: 31536000	0
monitor-hold-down-time	Time of day at which to fail back to primary after it re-establishes.	user	Not Specified	
monitor-hold-down-type	Recovery time method when primary interface re-establishes.	option	-	immediate
	<b>Option</b>	<b>Description</b>		
	<i>immediate</i>	Fail back immediately after primary recovers.		
	<i>delay</i>	Number of seconds to delay fail back after primary recovers.		
	<i>time</i>	Specify a time at which to fail back after primary recovers.		
monitor-hold-down-weekday	Day of the week to recover once primary re-establishes.	option	-	sunday
	<b>Option</b>	<b>Description</b>		
	<i>everyday</i>	Every Day.		

Parameter	Description	Type	Size	Default
	<div>OptionDescription</div>			
	<i>sunday</i>	Sunday.		
	<i>monday</i>	Monday.		
	<i>tuesday</i>	Tuesday.		
	<i>wednesday</i>	Wednesday.		
	<i>thursday</i>	Thursday.		
	<i>friday</i>	Friday.		
	<i>saturday</i>	Saturday.		
name	IPsec remote gateway name.	string	Maximum length: 15	
nattraversal	Enable/disable NAT traversal.	option	-	enable
	<div>OptionDescription</div>			
	<i>enable</i>	Enable IPsec NAT traversal.		
	<i>disable</i>	Disable IPsec NAT traversal.		
	<i>forced</i>	Force IPsec NAT traversal on.		
negotiate-timeout	IKE SA negotiation timeout in seconds.	integer	Minimum value: 1 Maximum value: 300	30
net-device	Enable/disable kernel device creation.	option	-	disable
	<div>OptionDescription</div>			
	<i>enable</i>	Create a kernel device for every tunnel.		
	<i>disable</i>	Do not create a kernel device for tunnels.		
network-id	VPN gateway network ID.	integer	Minimum value: 0 Maximum value: 255	0
network-overlay	Enable/disable network overlays.	option	-	disable
	<div>OptionDescription</div>			
	<i>disable</i>	Disable network overlays.		
	<i>enable</i>	Enable network overlays.		

Parameter	Description	Type	Size	Default
npu-offload *	Enable/disable offloading NPU.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable NPU offloading.		
	<i>disable</i>	Disable NPU offloading.		
passive-mode	Enable/disable IPsec passive mode for static tunnels.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable IPsec passive mode.		
	<i>disable</i>	Disable IPsec passive mode.		
peer	Accept this peer certificate.	string	Maximum length: 35	
peergrp	Accept this peer certificate group.	string	Maximum length: 35	
peerid	Accept this peer identity.	string	Maximum length: 255	
peertype	Accept this peer type.	option	-	peer
	<b>Option</b>	<b>Description</b>		
	<i>any</i>	Accept any peer ID.		
	<i>one</i>	Accept this peer ID.		
	<i>dialup</i>	Accept peer ID in dialup group.		
	<i>peer</i>	Accept this peer certificate.		
	<i>peergrp</i>	Accept this peer certificate group.		
ppk	Enable/disable IKEv2 Postquantum Preshared Key (PPK).	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable use of IKEv2 Postquantum Preshared Key (PPK).		
	<i>allow</i>	Allow, but do not require, use of IKEv2 Postquantum Preshared Key (PPK).		
	<i>require</i>	Require use of IKEv2 Postquantum Preshared Key (PPK).		
ppk-identity	IKEv2 Postquantum Preshared Key Identity.	string	Maximum length: 35	

Parameter	Description	Type	Size	Default																																														
ppk-secret	IKEv2 Postquantum Preshared Key (ASCII string or hexadecimal encoded with a leading 0x).	password-3	Not Specified																																															
priority	Priority for routes added by IKE.	integer	Minimum value: 1 Maximum value: 65535	1																																														
proposal	Phase1 proposal.	option	-																																															
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>des-md5</td><td>des-md5</td></tr><tr><td>des-sha1</td><td>des-sha1</td></tr><tr><td>des-sha256</td><td>des-sha256</td></tr><tr><td>des-sha384</td><td>des-sha384</td></tr><tr><td>des-sha512</td><td>des-sha512</td></tr><tr><td>3des-md5</td><td>3des-md5</td></tr><tr><td>3des-sha1</td><td>3des-sha1</td></tr><tr><td>3des-sha256</td><td>3des-sha256</td></tr><tr><td>3des-sha384</td><td>3des-sha384</td></tr><tr><td>3des-sha512</td><td>3des-sha512</td></tr><tr><td>aes128-md5</td><td>aes128-md5</td></tr><tr><td>aes128-sha1</td><td>aes128-sha1</td></tr><tr><td>aes128-sha256</td><td>aes128-sha256</td></tr><tr><td>aes128-sha384</td><td>aes128-sha384</td></tr><tr><td>aes128-sha512</td><td>aes128-sha512</td></tr><tr><td>aes128gcm-prfsha1</td><td>aes128gcm-prfsha1</td></tr><tr><td>aes128gcm-prfsha256</td><td>aes128gcm-prfsha256</td></tr><tr><td>aes128gcm-prfsha384</td><td>aes128gcm-prfsha384</td></tr><tr><td>aes128gcm-prfsha512</td><td>aes128gcm-prfsha512</td></tr><tr><td>aes192-md5</td><td>aes192-md5</td></tr><tr><td>aes192-sha1</td><td>aes192-sha1</td></tr><tr><td>aes192-sha256</td><td>aes192-sha256</td></tr></table>				Option	Description	des-md5	des-md5	des-sha1	des-sha1	des-sha256	des-sha256	des-sha384	des-sha384	des-sha512	des-sha512	3des-md5	3des-md5	3des-sha1	3des-sha1	3des-sha256	3des-sha256	3des-sha384	3des-sha384	3des-sha512	3des-sha512	aes128-md5	aes128-md5	aes128-sha1	aes128-sha1	aes128-sha256	aes128-sha256	aes128-sha384	aes128-sha384	aes128-sha512	aes128-sha512	aes128gcm-prfsha1	aes128gcm-prfsha1	aes128gcm-prfsha256	aes128gcm-prfsha256	aes128gcm-prfsha384	aes128gcm-prfsha384	aes128gcm-prfsha512	aes128gcm-prfsha512	aes192-md5	aes192-md5	aes192-sha1	aes192-sha1	aes192-sha256	aes192-sha256
	Option	Description																																																
	des-md5	des-md5																																																
	des-sha1	des-sha1																																																
	des-sha256	des-sha256																																																
	des-sha384	des-sha384																																																
	des-sha512	des-sha512																																																
	3des-md5	3des-md5																																																
	3des-sha1	3des-sha1																																																
	3des-sha256	3des-sha256																																																
	3des-sha384	3des-sha384																																																
	3des-sha512	3des-sha512																																																
	aes128-md5	aes128-md5																																																
	aes128-sha1	aes128-sha1																																																
	aes128-sha256	aes128-sha256																																																
	aes128-sha384	aes128-sha384																																																
	aes128-sha512	aes128-sha512																																																
	aes128gcm-prfsha1	aes128gcm-prfsha1																																																
	aes128gcm-prfsha256	aes128gcm-prfsha256																																																
	aes128gcm-prfsha384	aes128gcm-prfsha384																																																
	aes128gcm-prfsha512	aes128gcm-prfsha512																																																
	aes192-md5	aes192-md5																																																
	aes192-sha1	aes192-sha1																																																
	aes192-sha256	aes192-sha256																																																



Parameter	Description	Type	Size	Default
	Option		Description	
	<i>aes192-sha384</i>		aes192-sha384	
	<i>aes192-sha512</i>		aes192-sha512	
	<i>aes256-md5</i>		aes256-md5	
	<i>aes256-sha1</i>		aes256-sha1	
	<i>aes256-sha256</i>		aes256-sha256	
	<i>aes256-sha384</i>		aes256-sha384	
	<i>aes256-sha512</i>		aes256-sha512	
	<i>aes256gcm-prfsha1</i>		aes256gcm-prfsha1	
	<i>aes256gcm-prfsha256</i>		aes256gcm-prfsha256	
	<i>aes256gcm-prfsha384</i>		aes256gcm-prfsha384	
	<i>aes256gcm-prfsha512</i>		aes256gcm-prfsha512	
	<i>chacha20poly1305-prfsha1</i>		chacha20poly1305-prfsha1	
	<i>chacha20poly1305-prfsha256</i>		chacha20poly1305-prfsha256	
	<i>chacha20poly1305-prfsha384</i>		chacha20poly1305-prfsha384	
	<i>chacha20poly1305-prfsha512</i>		chacha20poly1305-prfsha512	
	<i>aria128-md5</i>		aria128-md5	
	<i>aria128-sha1</i>		aria128-sha1	
	<i>aria128-sha256</i>		aria128-sha256	
	<i>aria128-sha384</i>		aria128-sha384	
	<i>aria128-sha512</i>		aria128-sha512	
	<i>aria192-md5</i>		aria192-md5	
	<i>aria192-sha1</i>		aria192-sha1	
	<i>aria192-sha256</i>		aria192-sha256	
	<i>aria192-sha384</i>		aria192-sha384	
	<i>aria192-sha512</i>		aria192-sha512	
	<i>aria256-md5</i>		aria256-md5	
	<i>aria256-sha1</i>		aria256-sha1	
	<i>aria256-sha256</i>		aria256-sha256	
	<i>aria256-sha384</i>		aria256-sha384	

Parameter	Description	Type	Size	Default															
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>aria256-sha512</i></td><td>aria256-sha512</td></tr><tr><td><i>seed-md5</i></td><td>seed-md5</td></tr><tr><td><i>seed-sha1</i></td><td>seed-sha1</td></tr><tr><td><i>seed-sha256</i></td><td>seed-sha256</td></tr><tr><td><i>seed-sha384</i></td><td>seed-sha384</td></tr><tr><td><i>seed-sha512</i></td><td>seed-sha512</td></tr></table>		Option	Description	<i>aria256-sha512</i>	aria256-sha512	<i>seed-md5</i>	seed-md5	<i>seed-sha1</i>	seed-sha1	<i>seed-sha256</i>	seed-sha256	<i>seed-sha384</i>	seed-sha384	<i>seed-sha512</i>	seed-sha512			
	Option	Description																	
	<i>aria256-sha512</i>	aria256-sha512																	
	<i>seed-md5</i>	seed-md5																	
	<i>seed-sha1</i>	seed-sha1																	
	<i>seed-sha256</i>	seed-sha256																	
	<i>seed-sha384</i>	seed-sha384																	
<i>seed-sha512</i>	seed-sha512																		
psksecret	Pre-shared secret for PSK authentication (ASCII string or hexadecimal encoded with a leading 0x).	password-3	Not Specified																
psksecret-remote	Pre-shared secret for remote side PSK authentication (ASCII string or hexadecimal encoded with a leading 0x).	password-3	Not Specified																
reauth	Enable/disable re-authentication upon IKE SA lifetime expiration.	option	-	disable															
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable IKE SA re-authentication.</td></tr><tr><td><i>enable</i></td><td>Enable IKE SA re-authentication.</td></tr></table>		Option	Description	<i>disable</i>	Disable IKE SA re-authentication.	<i>enable</i>	Enable IKE SA re-authentication.											
	Option	Description																	
	<i>disable</i>	Disable IKE SA re-authentication.																	
<i>enable</i>	Enable IKE SA re-authentication.																		
rekey	Enable/disable phase1 rekey.	option	-	enable															
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable phase1 rekey.</td></tr><tr><td><i>disable</i></td><td>Disable phase1 rekey.</td></tr></table>		Option	Description	<i>enable</i>	Enable phase1 rekey.	<i>disable</i>	Disable phase1 rekey.											
	Option	Description																	
	<i>enable</i>	Enable phase1 rekey.																	
<i>disable</i>	Disable phase1 rekey.																		
remote-gw	IPv4 address of the remote gateway's external interface.	ipv4-address	Not Specified	0.0.0.0															
remote-gw6	IPv6 address of the remote gateway's external interface.	ipv6-address	Not Specified	::															
remotegw-ddns	Domain name of remote gateway. For example, name.ddns.com.	string	Maximum length: 63																
rsa-signature-format	Digital Signature Authentication RSA signature format.	option	-	pkcs1															

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>pkcs1</i>	RSASSA PKCS#1 v1.5.		
	<i>pss</i>	RSASSA Probabilistic Signature Scheme (PSS).		
save-password	Enable/disable saving XAuth username and password on VPN clients.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable saving XAuth username and password on VPN clients.		
	<i>enable</i>	Enable saving XAuth username and password on VPN clients.		
send-cert-chain	Enable/disable sending certificate chain.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable sending certificate chain.		
	<i>disable</i>	Disable sending certificate chain.		
signature-hash-alg	Digital Signature Authentication hash algorithms.	option	-	sha2-512
	<b>Option</b>	<b>Description</b>		
	<i>sha1</i>	SHA1.		
	<i>sha2-256</i>	SHA2-256.		
	<i>sha2-384</i>	SHA2-384.		
	<i>sha2-512</i>	SHA2-512.		
split-include-service	Split-include services.	string	Maximum length: 79	
suite-b	Use Suite-B.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Do not use UI suite.		
	<i>suite-b-gcm-128</i>	Use Suite-B-GCM-128.		
	<i>suite-b-gcm-256</i>	Use Suite-B-GCM-256.		
type	Remote gateway type.	option	-	static

Parameter	Description	Type	Size	Default																								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>static</i></td><td>Remote VPN gateway has fixed IP address.</td></tr><tr><td><i>dynamic</i></td><td>Remote VPN gateway has dynamic IP address.</td></tr><tr><td><i>ddns</i></td><td>Remote VPN gateway has dynamic IP address and is a dynamic DNS client.</td></tr></table>	Option	Description	<i>static</i>	Remote VPN gateway has fixed IP address.	<i>dynamic</i>	Remote VPN gateway has dynamic IP address.	<i>ddns</i>	Remote VPN gateway has dynamic IP address and is a dynamic DNS client.																			
	Option	Description																										
	<i>static</i>	Remote VPN gateway has fixed IP address.																										
	<i>dynamic</i>	Remote VPN gateway has dynamic IP address.																										
<i>ddns</i>	Remote VPN gateway has dynamic IP address and is a dynamic DNS client.																											
unity-support	Enable/disable support for Cisco UNITY Configuration Method extensions.	option	-	enable																								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable Cisco Unity Configuration Method Extensions.</td></tr><tr><td><i>enable</i></td><td>Enable Cisco Unity Configuration Method Extensions.</td></tr></table>	Option	Description	<i>disable</i>	Disable Cisco Unity Configuration Method Extensions.	<i>enable</i>	Enable Cisco Unity Configuration Method Extensions.																					
	Option	Description																										
	<i>disable</i>	Disable Cisco Unity Configuration Method Extensions.																										
<i>enable</i>	Enable Cisco Unity Configuration Method Extensions.																											
usrgrp	User group name for dialup peers.	string	Maximum length: 35																									
vni	VNI of VXLAN tunnel.	integer	Minimum value: 1 Maximum value: 16777215	0																								
wizard-type	GUI VPN Wizard Type.	option	-	custom																								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>custom</i></td><td>Custom VPN configuration.</td></tr><tr><td><i>dialup-forticlient</i></td><td>Dial Up - FortiClient Windows, Mac and Android.</td></tr><tr><td><i>dialup-ios</i></td><td>Dial Up - iPhone / iPad Native IPsec Client.</td></tr><tr><td><i>dialup-android</i></td><td>Dial Up - Android Native IPsec Client.</td></tr><tr><td><i>dialup-windows</i></td><td>Dial Up - Windows Native IPsec Client.</td></tr><tr><td><i>dialup-cisco</i></td><td>Dial Up - Cisco IPsec Client.</td></tr><tr><td><i>static-fortigate</i></td><td>Site to Site - FortiGate.</td></tr><tr><td><i>dialup-fortigate</i></td><td>Dial Up - FortiGate.</td></tr><tr><td><i>static-cisco</i></td><td>Site to Site - Cisco.</td></tr><tr><td><i>dialup-cisco-fw</i></td><td>Dialup Up - Cisco Firewall.</td></tr><tr><td><i>simplified-static-fortigate</i></td><td>Site to Site - FortiGate (SD-WAN).</td></tr></table>	Option	Description	<i>custom</i>	Custom VPN configuration.	<i>dialup-forticlient</i>	Dial Up - FortiClient Windows, Mac and Android.	<i>dialup-ios</i>	Dial Up - iPhone / iPad Native IPsec Client.	<i>dialup-android</i>	Dial Up - Android Native IPsec Client.	<i>dialup-windows</i>	Dial Up - Windows Native IPsec Client.	<i>dialup-cisco</i>	Dial Up - Cisco IPsec Client.	<i>static-fortigate</i>	Site to Site - FortiGate.	<i>dialup-fortigate</i>	Dial Up - FortiGate.	<i>static-cisco</i>	Site to Site - Cisco.	<i>dialup-cisco-fw</i>	Dialup Up - Cisco Firewall.	<i>simplified-static-fortigate</i>	Site to Site - FortiGate (SD-WAN).			
	Option	Description																										
	<i>custom</i>	Custom VPN configuration.																										
	<i>dialup-forticlient</i>	Dial Up - FortiClient Windows, Mac and Android.																										
	<i>dialup-ios</i>	Dial Up - iPhone / iPad Native IPsec Client.																										
	<i>dialup-android</i>	Dial Up - Android Native IPsec Client.																										
	<i>dialup-windows</i>	Dial Up - Windows Native IPsec Client.																										
	<i>dialup-cisco</i>	Dial Up - Cisco IPsec Client.																										
	<i>static-fortigate</i>	Site to Site - FortiGate.																										
	<i>dialup-fortigate</i>	Dial Up - FortiGate.																										
	<i>static-cisco</i>	Site to Site - Cisco.																										
	<i>dialup-cisco-fw</i>	Dialup Up - Cisco Firewall.																										
<i>simplified-static-fortigate</i>	Site to Site - FortiGate (SD-WAN).																											

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>hub-fortigate-auto-discovery</i>	Hub role in a Hub-and-Spoke auto-discovery VPN.		
	<i>spoke-fortigate-auto-discovery</i>	Spoke role in a Hub-and-Spoke auto-discovery VPN.		
xauthtype	XAuth type.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable.		
	<i>client</i>	Enable as client.		
	<i>pap</i>	Enable as server PAP.		
	<i>chap</i>	Enable as server CHAP.		
	<i>auto</i>	Enable as server auto.		

\* This parameter may not exist in some models.

### config ipv4-exclude-range

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
start-ip	Start of IPv4 exclusive range.	ipv4-address	Not Specified	0.0.0.0
end-ip	End of IPv4 exclusive range.	ipv4-address	Not Specified	0.0.0.0

### config ipv6-exclude-range

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0

Parameter	Description	Type	Size	Default
start-ip	Start of IPv6 exclusive range.	ipv6-address	Not Specified	::
end-ip	End of IPv6 exclusive range.	ipv6-address	Not Specified	::

## config vpn ipsec phase1

Configure VPN remote gateway.

```

config vpn ipsec phase1
    Description: Configure VPN remote gateway.
    edit <name>
        set acct-verify [enable|disable]
        set add-gw-route [enable|disable]
        set add-route [disable|enable]
        set assign-ip [disable|enable]
        set assign-ip-from [range|usrgrp|...]
        set authmethod [psk|signature]
        set authmethod-remote [psk|signature]
        set authpasswd {password}
        set authusr {string}
        set authusrgrp {string}
        set auto-negotiate [enable|disable]
        set backup-gateway <address1>, <address2>, ...
        set banner {var-string}
        set cert-id-validation [enable|disable]
        set certificate <name1>, <name2>, ...
        set childless-ike [enable|disable]
        set client-auto-negotiate [disable|enable]
        set client-keep-alive [disable|enable]
        set comments {var-string}
        set dhcp-ra-giaddr {ipv4-address}
        set dhcp6-ra-linkaddr {ipv6-address}
        set dhgrp {option1}, {option2}, ...
        set digital-signature-auth [enable|disable]
        set distance {integer}
        set dns-mode [manual|auto]
        set domain {string}
        set dpd [disable|on-idle|...]
        set dpd-retrycount {integer}
        set dpd-retryinterval {user}
        set eap [enable|disable]
        set eap-exclude-peergrp {string}
        set eap-identity [use-id-payload|send-request]
        set enforce-unique-id [disable|keep-new|...]
        set esn [require|allow|...]
        set fec-base {integer}
        set fec-codec [rs|xor]
        set fec-egress [enable|disable]
        set fec-health-check {string}
        set fec-ingress [enable|disable]
        set fec-mapping-profile {string}

```

```

set fec-receive-timeout {integer}
set fec-redundant {integer}
set fec-send-timeout {integer}
set fgsp-sync [enable|disable]
set forticlient-enforcement [enable|disable]
set fragmentation [enable|disable]
set fragmentation-mtu {integer}
set group-authentication [enable|disable]
set group-authentication-secret {password-3}
set ha-sync-esp-seqno [enable|disable]
set idle-timeout [enable|disable]
set idle-timeoutinterval {integer}
set ike-version [1|2]
set inbound-dscp-copy [enable|disable]
set include-local-lan [disable|enable]
set interface {string}
set ip-delay-interval {integer}
set ipv4-dns-server1 {ipv4-address}
set ipv4-dns-server2 {ipv4-address}
set ipv4-dns-server3 {ipv4-address}
set ipv4-end-ip {ipv4-address}
config ipv4-exclude-range
    Description: Configuration Method IPv4 exclude ranges.
    edit <id>
        set start-ip {ipv4-address}
        set end-ip {ipv4-address}
    next
end
set ipv4-name {string}
set ipv4-netmask {ipv4-netmask}
set ipv4-split-exclude {string}
set ipv4-split-include {string}
set ipv4-start-ip {ipv4-address}
set ipv4-wins-server1 {ipv4-address}
set ipv4-wins-server2 {ipv4-address}
set ipv6-dns-server1 {ipv6-address}
set ipv6-dns-server2 {ipv6-address}
set ipv6-dns-server3 {ipv6-address}
set ipv6-end-ip {ipv6-address}
config ipv6-exclude-range
    Description: Configuration method IPv6 exclude ranges.
    edit <id>
        set start-ip {ipv6-address}
        set end-ip {ipv6-address}
    next
end
set ipv6-name {string}
set ipv6-prefix {integer}
set ipv6-split-exclude {string}
set ipv6-split-include {string}
set ipv6-start-ip {ipv6-address}
set keepalive {integer}
set keylife {integer}
set local-gw {ipv4-address}
set localid {string}
set localid-type [auto|fqdn|...]

```

```

set mesh-selector-type [disable|subnet|...]
set mode [aggressive|main]
set mode-cfg [disable|enable]
set nattraversal [enable|disable|...]
set negotiate-timeout {integer}
set npu-offload [enable|disable]
set peer {string}
set peergrp {string}
set peerid {string}
set peertype [any|one|...]
set ppk [disable|allow|...]
set ppk-identity {string}
set ppk-secret {password-3}
set priority {integer}
set proposal {option1}, {option2}, ...
set psksecret {password-3}
set psksecret-remote {password-3}
set reauth [disable|enable]
set rekey [enable|disable]
set remote-gw {ipv4-address}
set remotegw-ddns {string}
set rsa-signature-format [pkcs1|pss]
set save-password [disable|enable]
set send-cert-chain [enable|disable]
set signature-hash-alg {option1}, {option2}, ...
set split-include-service {string}
set suite-b [disable|suite-b-gcm-128|...]
set type [static|dynamic|...]
set unity-support [disable|enable]
set usrgrp {string}
set wizard-type [custom|dialup-forticlient|...]
set xauthtype [disable|client|...]

```

next

end

## config vpn ipsec phase1

Parameter	Description	Type	Size	Default
acct-verify	Enable/disable verification of RADIUS accounting record.	option	-	disable
	Option	Description		
	enable	Enable verification of RADIUS accounting record.		
	disable	Disable verification of RADIUS accounting record.		
add-gw-route	Enable/disable automatically add a route to the remote gateway.	option	-	disable



Parameter	Description	Type	Size	Default
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Automatically add a route to the remote gateway.		
	<i>disable</i>	Do not automatically add a route to the remote gateway.		
add-route	Enable/disable control addition of a route to peer destination selector.	option	-	disable
	<b>Option</b> <b>Description</b>			
	<i>disable</i>	Do not add a route to destination of peer selector.		
	<i>enable</i>	Add route to destination of peer selector.		
assign-ip	Enable/disable assignment of IP to IPsec interface via configuration method.	option	-	enable
	<b>Option</b> <b>Description</b>			
	<i>disable</i>	Do not assign an IP address to the IPsec interface.		
	<i>enable</i>	Assign an IP address to the IPsec interface.		
assign-ip-from	Method by which the IP address will be assigned.	option	-	range
	<b>Option</b> <b>Description</b>			
	<i>range</i>	Assign IP address from locally defined range.		
	<i>usrgrp</i>	Assign IP address via user group.		
	<i>dhcp</i>	Assign IP address via DHCP.		
	<i>name</i>	Assign IP address from firewall address or group.		
authmethod	Authentication method.	option	-	psk
	<b>Option</b> <b>Description</b>			
	<i>psk</i>	PSK authentication method.		
	<i>signature</i>	Signature authentication method.		
authmethod-remote	Authentication method (remote side).	option	-	
	<b>Option</b> <b>Description</b>			
	<i>psk</i>	PSK authentication method.		
	<i>signature</i>	Signature authentication method.		

Parameter	Description	Type	Size	Default						
authpasswd	XAuth password (max 35 characters).	password	Not Specified							
authusr	XAuth user name.	string	Maximum length: 64							
authusrgrp	Authentication user group.	string	Maximum length: 35							
auto-negotiate	Enable/disable automatic initiation of IKE SA negotiation.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable automatic initiation of IKE SA negotiation.</td></tr><tr><td><i>disable</i></td><td>Disable automatic initiation of IKE SA negotiation.</td></tr></table>				Option	Description	<i>enable</i>	Enable automatic initiation of IKE SA negotiation.	<i>disable</i>	Disable automatic initiation of IKE SA negotiation.
	Option	Description								
	<i>enable</i>	Enable automatic initiation of IKE SA negotiation.								
<i>disable</i>	Disable automatic initiation of IKE SA negotiation.									
backup-gateway <address>	Instruct unity clients about the backup gateway address(es). Address of backup gateway.	string	Maximum length: 79							
banner	Message that unity client should display after connecting.	var-string	Maximum length: 1024							
cert-id-validation	Enable/disable cross validation of peer ID and the identity in the peer's certificate as specified in RFC 4945.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable cross validation of peer ID and the identity in the peer's certificate as specified in RFC 4945.</td></tr><tr><td><i>disable</i></td><td>Disable cross validation of peer ID and the identity in the peer's certificate as specified in RFC 4945.</td></tr></table>				Option	Description	<i>enable</i>	Enable cross validation of peer ID and the identity in the peer's certificate as specified in RFC 4945.	<i>disable</i>	Disable cross validation of peer ID and the identity in the peer's certificate as specified in RFC 4945.
	Option	Description								
	<i>enable</i>	Enable cross validation of peer ID and the identity in the peer's certificate as specified in RFC 4945.								
<i>disable</i>	Disable cross validation of peer ID and the identity in the peer's certificate as specified in RFC 4945.									
certificate <name>	Names of up to 4 signed personal certificates. Certificate name.	string	Maximum length: 79							
childless-ike	Enable/disable childless IKEv2 initiation (RFC 6023).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable childless IKEv2 initiation (RFC 6023).</td></tr><tr><td><i>disable</i></td><td>Disable childless IKEv2 initiation (RFC 6023).</td></tr></table>				Option	Description	<i>enable</i>	Enable childless IKEv2 initiation (RFC 6023).	<i>disable</i>	Disable childless IKEv2 initiation (RFC 6023).
	Option	Description								
	<i>enable</i>	Enable childless IKEv2 initiation (RFC 6023).								
<i>disable</i>	Disable childless IKEv2 initiation (RFC 6023).									
client-auto-negotiate	Enable/disable allowing the VPN client to bring up the tunnel when there is no traffic.	option	-	disable						

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable allowing the VPN client to bring up the tunnel when there is no traffic.		
	<i>enable</i>	Enable allowing the VPN client to bring up the tunnel when there is no traffic.		
client-keep-alive	Enable/disable allowing the VPN client to keep the tunnel up when there is no traffic.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable allowing the VPN client to keep the tunnel up when there is no traffic.		
	<i>enable</i>	Enable allowing the VPN client to keep the tunnel up when there is no traffic.		
comments	Comment.	var-string	Maximum length: 255	
dhcp-ra-giaddr	Relay agent gateway IP address to use in the giaddr field of DHCP requests.	ipv4-address	Not Specified	0.0.0.0
dhcp6-ra-linkaddr	Relay agent IPv6 link address to use in DHCP6 requests.	ipv6-address	Not Specified	::
dhgrp	DH group.	option	-	14
	<b>Option</b>	<b>Description</b>		
	1	DH Group 1.		
	2	DH Group 2.		
	5	DH Group 5.		
	14	DH Group 14.		
	15	DH Group 15.		
	16	DH Group 16.		
	17	DH Group 17.		
	18	DH Group 18.		
	19	DH Group 19.		
	20	DH Group 20.		
	21	DH Group 21.		

Parameter	Description	Type	Size	Default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>27</td><td>DH Group 27.</td></tr><tr><td>28</td><td>DH Group 28.</td></tr><tr><td>29</td><td>DH Group 29.</td></tr><tr><td>30</td><td>DH Group 30.</td></tr><tr><td>31</td><td>DH Group 31.</td></tr><tr><td>32</td><td>DH Group 32.</td></tr></table>	Option	Description	27	DH Group 27.	28	DH Group 28.	29	DH Group 29.	30	DH Group 30.	31	DH Group 31.	32	DH Group 32.			
	Option	Description																
	27	DH Group 27.																
	28	DH Group 28.																
	29	DH Group 29.																
	30	DH Group 30.																
	31	DH Group 31.																
32	DH Group 32.																	
digital-signature-auth	Enable/disable IKEv2 Digital Signature Authentication (RFC 7427).	option	-	disable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable IKEv2 Digital Signature Authentication (RFC 7427).</td></tr><tr><td>disable</td><td>Disable IKEv2 Digital Signature Authentication (RFC 7427).</td></tr></table>	Option	Description	enable	Enable IKEv2 Digital Signature Authentication (RFC 7427).	disable	Disable IKEv2 Digital Signature Authentication (RFC 7427).											
	Option	Description																
	enable	Enable IKEv2 Digital Signature Authentication (RFC 7427).																
disable	Disable IKEv2 Digital Signature Authentication (RFC 7427).																	
distance	Distance for routes added by IKE.	integer	Minimum value: 1 Maximum value: 255	15														
dns-mode	DNS server mode.	option	-	manual														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>manual</td><td>Manually configure DNS servers.</td></tr><tr><td>auto</td><td>Use default DNS servers.</td></tr></table>	Option	Description	manual	Manually configure DNS servers.	auto	Use default DNS servers.											
	Option	Description																
	manual	Manually configure DNS servers.																
auto	Use default DNS servers.																	
domain	Instruct unity clients about the single default DNS domain.	string	Maximum length: 63															
dpd	Dead Peer Detection mode.	option	-	on-demand														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable Dead Peer Detection.</td></tr><tr><td>on-idle</td><td>Trigger Dead Peer Detection when IPsec is idle.</td></tr><tr><td>on-demand</td><td>Trigger Dead Peer Detection when IPsec traffic is sent but no reply is received from the peer.</td></tr></table>	Option	Description	disable	Disable Dead Peer Detection.	on-idle	Trigger Dead Peer Detection when IPsec is idle.	on-demand	Trigger Dead Peer Detection when IPsec traffic is sent but no reply is received from the peer.									
	Option	Description																
	disable	Disable Dead Peer Detection.																
	on-idle	Trigger Dead Peer Detection when IPsec is idle.																
on-demand	Trigger Dead Peer Detection when IPsec traffic is sent but no reply is received from the peer.																	
dpd-retrycount	Number of DPD retry attempts.	integer	Minimum value: 0 Maximum value: 10	3														

Parameter	Description	Type	Size	Default								
dpd-retryinterval	DPD retry interval.	user	Not Specified									
eap	Enable/disable IKEv2 EAP authentication.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable IKEv2 EAP authentication.</td></tr><tr><td><i>disable</i></td><td>Disable IKEv2 EAP authentication.</td></tr></table>				Option	Description	<i>enable</i>	Enable IKEv2 EAP authentication.	<i>disable</i>	Disable IKEv2 EAP authentication.		
	Option	Description										
	<i>enable</i>	Enable IKEv2 EAP authentication.										
<i>disable</i>	Disable IKEv2 EAP authentication.											
eap-exclude-peergrp	Peer group excluded from EAP authentication.	string	Maximum length: 35									
eap-identity	IKEv2 EAP peer identity type.	option	-	use-id-payload								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>use-id-payload</i></td><td>Use IKEv2 IDi payload to resolve peer identity.</td></tr><tr><td><i>send-request</i></td><td>Use EAP identity request to resolve peer identity.</td></tr></table>				Option	Description	<i>use-id-payload</i>	Use IKEv2 IDi payload to resolve peer identity.	<i>send-request</i>	Use EAP identity request to resolve peer identity.		
	Option	Description										
	<i>use-id-payload</i>	Use IKEv2 IDi payload to resolve peer identity.										
<i>send-request</i>	Use EAP identity request to resolve peer identity.											
enforce-unique-id	Enable/disable peer ID uniqueness check.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable peer ID uniqueness enforcement.</td></tr><tr><td><i>keep-new</i></td><td>Enforce peer ID uniqueness, keep new connection if collision found.</td></tr><tr><td><i>keep-old</i></td><td>Enforce peer ID uniqueness, keep old connection if collision found.</td></tr></table>				Option	Description	<i>disable</i>	Disable peer ID uniqueness enforcement.	<i>keep-new</i>	Enforce peer ID uniqueness, keep new connection if collision found.	<i>keep-old</i>	Enforce peer ID uniqueness, keep old connection if collision found.
	Option	Description										
	<i>disable</i>	Disable peer ID uniqueness enforcement.										
	<i>keep-new</i>	Enforce peer ID uniqueness, keep new connection if collision found.										
<i>keep-old</i>	Enforce peer ID uniqueness, keep old connection if collision found.											
esn *	Extended sequence number (ESN) negotiation.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>require</i></td><td>Require extended sequence number.</td></tr><tr><td><i>allow</i></td><td>Allow extended sequence number.</td></tr><tr><td><i>disable</i></td><td>Disable extended sequence number.</td></tr></table>				Option	Description	<i>require</i>	Require extended sequence number.	<i>allow</i>	Allow extended sequence number.	<i>disable</i>	Disable extended sequence number.
	Option	Description										
	<i>require</i>	Require extended sequence number.										
	<i>allow</i>	Allow extended sequence number.										
<i>disable</i>	Disable extended sequence number.											
fec-base	Number of base Forward Error Correction packets.	integer	Minimum value: 1 Maximum value: 20	10								
fec-codec	Forward Error Correction encoding/decoding algorithm.	option	-	rs								

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>rs</td><td>Reed-Solomon FEC algorithm.</td></tr><tr><td>xor</td><td>XOR FEC algorithm.</td></tr></table>	Option	Description	rs	Reed-Solomon FEC algorithm.	xor	XOR FEC algorithm.			
	Option	Description								
	rs	Reed-Solomon FEC algorithm.								
xor	XOR FEC algorithm.									
fec-egress	Enable/disable Forward Error Correction for egress IPsec traffic.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable Forward Error Correction for egress IPsec traffic.</td></tr><tr><td>disable</td><td>Disable Forward Error Correction for egress IPsec traffic.</td></tr></table>	Option	Description	enable	Enable Forward Error Correction for egress IPsec traffic.	disable	Disable Forward Error Correction for egress IPsec traffic.			
	Option	Description								
	enable	Enable Forward Error Correction for egress IPsec traffic.								
disable	Disable Forward Error Correction for egress IPsec traffic.									
fec-health-check	SD-WAN health check.	string	Maximum length: 35							
fec-ingress	Enable/disable Forward Error Correction for ingress IPsec traffic.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable Forward Error Correction for ingress IPsec traffic.</td></tr><tr><td>disable</td><td>Disable Forward Error Correction for ingress IPsec traffic.</td></tr></table>	Option	Description	enable	Enable Forward Error Correction for ingress IPsec traffic.	disable	Disable Forward Error Correction for ingress IPsec traffic.			
	Option	Description								
	enable	Enable Forward Error Correction for ingress IPsec traffic.								
disable	Disable Forward Error Correction for ingress IPsec traffic.									
fec-mapping-profile	Forward Error Correction (FEC) mapping profile.	string	Maximum length: 35							
fec-receive-timeout	Timeout in milliseconds before dropping Forward Error Correction packets.	integer	Minimum value: 1 Maximum value: 1000	50						
fec-redundant	Number of redundant Forward Error Correction packets.	integer	Minimum value: 1 Maximum value: 5	1						
fec-send-timeout	Timeout in milliseconds before sending Forward Error Correction packets.	integer	Minimum value: 1 Maximum value: 1000	5						
fgsp-sync	Enable/disable IPsec syncing of tunnels for FGSP IPsec.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable IPsec syncing of tunnels to other cluster members.</td></tr><tr><td>disable</td><td>Disable IPsec syncing of tunnels to other cluster members.</td></tr></table>	Option	Description	enable	Enable IPsec syncing of tunnels to other cluster members.	disable	Disable IPsec syncing of tunnels to other cluster members.			
	Option	Description								
	enable	Enable IPsec syncing of tunnels to other cluster members.								
disable	Disable IPsec syncing of tunnels to other cluster members.									

Parameter	Description	Type	Size	Default						
forticlient-enforcement	Enable/disable FortiClient enforcement.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable FortiClient enforcement.</td></tr><tr><td><i>disable</i></td><td>Disable FortiClient enforcement.</td></tr></table>	Option	Description	<i>enable</i>	Enable FortiClient enforcement.	<i>disable</i>	Disable FortiClient enforcement.			
Option	Description									
<i>enable</i>	Enable FortiClient enforcement.									
<i>disable</i>	Disable FortiClient enforcement.									
fragmentation	Enable/disable fragment IKE message on re-transmission.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable intra-IKE fragmentation support on re-transmission.</td></tr><tr><td><i>disable</i></td><td>Disable intra-IKE fragmentation support.</td></tr></table>	Option	Description	<i>enable</i>	Enable intra-IKE fragmentation support on re-transmission.	<i>disable</i>	Disable intra-IKE fragmentation support.			
Option	Description									
<i>enable</i>	Enable intra-IKE fragmentation support on re-transmission.									
<i>disable</i>	Disable intra-IKE fragmentation support.									
fragmentation-mtu	IKE fragmentation MTU.	integer	Minimum value: 500 Maximum value: 16000	1200						
group-authentication	Enable/disable IKEv2 IDi group authentication.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable IKEv2 IDi group authentication.</td></tr><tr><td><i>disable</i></td><td>Disable IKEv2 IDi group authentication.</td></tr></table>	Option	Description	<i>enable</i>	Enable IKEv2 IDi group authentication.	<i>disable</i>	Disable IKEv2 IDi group authentication.			
Option	Description									
<i>enable</i>	Enable IKEv2 IDi group authentication.									
<i>disable</i>	Disable IKEv2 IDi group authentication.									
group-authentication-secret	Password for IKEv2 ID group authentication. ASCII string or hexadecimal indicated by a leading 0x.	password-3	Not Specified							
ha-sync-esp-seqno	Enable/disable sequence number jump ahead for IPsec HA.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable HA syncing of ESP sequence numbers.</td></tr><tr><td><i>disable</i></td><td>Disable HA syncing of ESP sequence numbers.</td></tr></table>	Option	Description	<i>enable</i>	Enable HA syncing of ESP sequence numbers.	<i>disable</i>	Disable HA syncing of ESP sequence numbers.			
Option	Description									
<i>enable</i>	Enable HA syncing of ESP sequence numbers.									
<i>disable</i>	Disable HA syncing of ESP sequence numbers.									
idle-timeout	Enable/disable IPsec tunnel idle timeout.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable IPsec tunnel idle timeout.</td></tr><tr><td><i>disable</i></td><td>Disable IPsec tunnel idle timeout.</td></tr></table>	Option	Description	<i>enable</i>	Enable IPsec tunnel idle timeout.	<i>disable</i>	Disable IPsec tunnel idle timeout.			
Option	Description									
<i>enable</i>	Enable IPsec tunnel idle timeout.									
<i>disable</i>	Disable IPsec tunnel idle timeout.									

Parameter	Description	Type	Size	Default
idle-timeoutinterval	IPsec tunnel idle timeout in minutes.	integer	Minimum value: 5 Maximum value: 43200	15
ike-version	IKE protocol version.	option	-	1
	<b>Option</b>	<b>Description</b>		
	1	Use IKEv1 protocol.		
	2	Use IKEv2 protocol.		
inbound-dscp-copy	Enable/disable copying of the DSCP values in the ESP header to the inner IP Header.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	enable	Enable copying of the DSCP values in the ESP header to the inner IP Header.		
	disable	Disable copying of the DSCP values in the ESP header to the inner IP Header.		
include-local-lan	Enable/disable allow local LAN access on unity clients.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	disable	Disable local LAN access on Unity clients.		
	enable	Enable local LAN access on Unity clients.		
interface	Local physical, aggregate, or VLAN outgoing interface.	string	Maximum length: 35	
ip-delay-interval	IP address reuse delay interval in seconds.	integer	Minimum value: 0 Maximum value: 28800	0
ipv4-dns-server1	IPv4 DNS server 1.	ipv4-address	Not Specified	0.0.0.0
ipv4-dns-server2	IPv4 DNS server 2.	ipv4-address	Not Specified	0.0.0.0
ipv4-dns-server3	IPv4 DNS server 3.	ipv4-address	Not Specified	0.0.0.0
ipv4-end-ip	End of IPv4 range.	ipv4-address	Not Specified	0.0.0.0



Parameter	Description	Type	Size	Default
ipv4-name	IPv4 address name.	string	Maximum length: 79	
ipv4-netmask	IPv4 Netmask.	ipv4-netmask	Not Specified	255.255.255.255
ipv4-split-exclude	IPv4 subnets that should not be sent over the IPsec tunnel.	string	Maximum length: 79	
ipv4-split-include	IPv4 split-include subnets.	string	Maximum length: 79	
ipv4-start-ip	Start of IPv4 range.	ipv4-address	Not Specified	0.0.0.0
ipv4-wins-server1	WINS server 1.	ipv4-address	Not Specified	0.0.0.0
ipv4-wins-server2	WINS server 2.	ipv4-address	Not Specified	0.0.0.0
ipv6-dns-server1	IPv6 DNS server 1.	ipv6-address	Not Specified	::
ipv6-dns-server2	IPv6 DNS server 2.	ipv6-address	Not Specified	::
ipv6-dns-server3	IPv6 DNS server 3.	ipv6-address	Not Specified	::
ipv6-end-ip	End of IPv6 range.	ipv6-address	Not Specified	::
ipv6-name	IPv6 address name.	string	Maximum length: 79	
ipv6-prefix	IPv6 prefix.	integer	Minimum value: 1 Maximum value: 128	128
ipv6-split-exclude	IPv6 subnets that should not be sent over the IPsec tunnel.	string	Maximum length: 79	
ipv6-split-include	IPv6 split-include subnets.	string	Maximum length: 79	
ipv6-start-ip	Start of IPv6 range.	ipv6-address	Not Specified	::
keepalive	NAT-T keep alive interval.	integer	Minimum value: 10 Maximum value: 900	10

Parameter	Description	Type	Size	Default														
keylife	Time to wait in seconds before phase 1 encryption key expires.	integer	Minimum value: 120 Maximum value: 172800	86400														
local-gw	Local VPN gateway.	ipv4-address	Not Specified	0.0.0.0														
localid	Local ID.	string	Maximum length: 63															
localid-type	Local ID type.	option	-	auto														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>auto</td><td>Select ID type automatically.</td></tr><tr><td>fqdn</td><td>Use fully qualified domain name.</td></tr><tr><td>user-fqdn</td><td>Use user fully qualified domain name.</td></tr><tr><td>keyid</td><td>Use key-id string.</td></tr><tr><td>address</td><td>Use local IP address.</td></tr><tr><td>asn1dn</td><td>Use ASN.1 distinguished name.</td></tr></table>				Option	Description	auto	Select ID type automatically.	fqdn	Use fully qualified domain name.	user-fqdn	Use user fully qualified domain name.	keyid	Use key-id string.	address	Use local IP address.	asn1dn	Use ASN.1 distinguished name.
Option	Description																	
auto	Select ID type automatically.																	
fqdn	Use fully qualified domain name.																	
user-fqdn	Use user fully qualified domain name.																	
keyid	Use key-id string.																	
address	Use local IP address.																	
asn1dn	Use ASN.1 distinguished name.																	
mesh-selector-type	Add selectors containing subsets of the configuration depending on traffic.	option	-	disable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable.</td></tr><tr><td>subnet</td><td>Enable addition of matching subnet selector.</td></tr><tr><td>host</td><td>Enable addition of host to host selector.</td></tr></table>				Option	Description	disable	Disable.	subnet	Enable addition of matching subnet selector.	host	Enable addition of host to host selector.						
Option	Description																	
disable	Disable.																	
subnet	Enable addition of matching subnet selector.																	
host	Enable addition of host to host selector.																	
mode	ID protection mode used to establish a secure channel.	option	-	main														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>aggressive</td><td>Aggressive mode.</td></tr><tr><td>main</td><td>Main mode.</td></tr></table>				Option	Description	aggressive	Aggressive mode.	main	Main mode.								
Option	Description																	
aggressive	Aggressive mode.																	
main	Main mode.																	
mode-cfg	Enable/disable configuration method.	option	-	disable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable Configuration Method.</td></tr><tr><td>enable</td><td>Enable Configuration Method.</td></tr></table>				Option	Description	disable	Disable Configuration Method.	enable	Enable Configuration Method.								
Option	Description																	
disable	Disable Configuration Method.																	
enable	Enable Configuration Method.																	

Parameter	Description	Type	Size	Default
name	IPsec remote gateway name.	string	Maximum length: 35	
nattraversal	Enable/disable NAT traversal.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable IPsec NAT traversal.		
	<i>disable</i>	Disable IPsec NAT traversal.		
	<i>forced</i>	Force IPsec NAT traversal on.		
negotiate-timeout	IKE SA negotiation timeout in seconds.	integer	Minimum value: 1 Maximum value: 300	30
npu-offload *	Enable/disable offloading NPU.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable NPU offloading.		
	<i>disable</i>	Disable NPU offloading.		
peer	Accept this peer certificate.	string	Maximum length: 35	
peergrp	Accept this peer certificate group.	string	Maximum length: 35	
peerid	Accept this peer identity.	string	Maximum length: 255	
peertype	Accept this peer type.	option	-	peer
	<b>Option</b>	<b>Description</b>		
	<i>any</i>	Accept any peer ID.		
	<i>one</i>	Accept this peer ID.		
	<i>dialup</i>	Accept peer ID in dialup group.		
	<i>peer</i>	Accept this peer certificate.		
	<i>peergrp</i>	Accept this peer certificate group.		
ppk	Enable/disable IKEv2 Postquantum Preshared Key (PPK).	option	-	disable

Parameter	Description	Type	Size	Default																																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable use of IKEv2 Postquantum Preshared Key (PPK).</td></tr><tr><td><i>allow</i></td><td>Allow, but do not require, use of IKEv2 Postquantum Preshared Key (PPK).</td></tr><tr><td><i>require</i></td><td>Require use of IKEv2 Postquantum Preshared Key (PPK).</td></tr></table>	Option	Description	<i>disable</i>	Disable use of IKEv2 Postquantum Preshared Key (PPK).	<i>allow</i>	Allow, but do not require, use of IKEv2 Postquantum Preshared Key (PPK).	<i>require</i>	Require use of IKEv2 Postquantum Preshared Key (PPK).																													
	Option	Description																																				
	<i>disable</i>	Disable use of IKEv2 Postquantum Preshared Key (PPK).																																				
	<i>allow</i>	Allow, but do not require, use of IKEv2 Postquantum Preshared Key (PPK).																																				
<i>require</i>	Require use of IKEv2 Postquantum Preshared Key (PPK).																																					
ppk-identity	IKEv2 Postquantum Preshared Key Identity.	string	Maximum length: 35																																			
ppk-secret	IKEv2 Postquantum Preshared Key (ASCII string or hexadecimal encoded with a leading 0x).	password-3	Not Specified																																			
priority	Priority for routes added by IKE.	integer	Minimum value: 1 Maximum value: 65535	1																																		
proposal	Phase1 proposal.	option	-																																			
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>des-md5</i></td><td>des-md5</td></tr><tr><td><i>des-sha1</i></td><td>des-sha1</td></tr><tr><td><i>des-sha256</i></td><td>des-sha256</td></tr><tr><td><i>des-sha384</i></td><td>des-sha384</td></tr><tr><td><i>des-sha512</i></td><td>des-sha512</td></tr><tr><td><i>3des-md5</i></td><td>3des-md5</td></tr><tr><td><i>3des-sha1</i></td><td>3des-sha1</td></tr><tr><td><i>3des-sha256</i></td><td>3des-sha256</td></tr><tr><td><i>3des-sha384</i></td><td>3des-sha384</td></tr><tr><td><i>3des-sha512</i></td><td>3des-sha512</td></tr><tr><td><i>aes128-md5</i></td><td>aes128-md5</td></tr><tr><td><i>aes128-sha1</i></td><td>aes128-sha1</td></tr><tr><td><i>aes128-sha256</i></td><td>aes128-sha256</td></tr><tr><td><i>aes128-sha384</i></td><td>aes128-sha384</td></tr><tr><td><i>aes128-sha512</i></td><td>aes128-sha512</td></tr><tr><td><i>aes128gcm-prfsha1</i></td><td>aes128gcm-prfsha1</td></tr></table>	Option	Description	<i>des-md5</i>	des-md5	<i>des-sha1</i>	des-sha1	<i>des-sha256</i>	des-sha256	<i>des-sha384</i>	des-sha384	<i>des-sha512</i>	des-sha512	<i>3des-md5</i>	3des-md5	<i>3des-sha1</i>	3des-sha1	<i>3des-sha256</i>	3des-sha256	<i>3des-sha384</i>	3des-sha384	<i>3des-sha512</i>	3des-sha512	<i>aes128-md5</i>	aes128-md5	<i>aes128-sha1</i>	aes128-sha1	<i>aes128-sha256</i>	aes128-sha256	<i>aes128-sha384</i>	aes128-sha384	<i>aes128-sha512</i>	aes128-sha512	<i>aes128gcm-prfsha1</i>	aes128gcm-prfsha1			
	Option	Description																																				
	<i>des-md5</i>	des-md5																																				
	<i>des-sha1</i>	des-sha1																																				
	<i>des-sha256</i>	des-sha256																																				
	<i>des-sha384</i>	des-sha384																																				
	<i>des-sha512</i>	des-sha512																																				
	<i>3des-md5</i>	3des-md5																																				
	<i>3des-sha1</i>	3des-sha1																																				
	<i>3des-sha256</i>	3des-sha256																																				
	<i>3des-sha384</i>	3des-sha384																																				
	<i>3des-sha512</i>	3des-sha512																																				
	<i>aes128-md5</i>	aes128-md5																																				
	<i>aes128-sha1</i>	aes128-sha1																																				
	<i>aes128-sha256</i>	aes128-sha256																																				
	<i>aes128-sha384</i>	aes128-sha384																																				
	<i>aes128-sha512</i>	aes128-sha512																																				
	<i>aes128gcm-prfsha1</i>	aes128gcm-prfsha1																																				

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>aes128gcm-prfsha256</i>	aes128gcm-prfsha256		
	<i>aes128gcm-prfsha384</i>	aes128gcm-prfsha384		
	<i>aes128gcm-prfsha512</i>	aes128gcm-prfsha512		
	<i>aes192-md5</i>	aes192-md5		
	<i>aes192-sha1</i>	aes192-sha1		
	<i>aes192-sha256</i>	aes192-sha256		
	<i>aes192-sha384</i>	aes192-sha384		
	<i>aes192-sha512</i>	aes192-sha512		
	<i>aes256-md5</i>	aes256-md5		
	<i>aes256-sha1</i>	aes256-sha1		
	<i>aes256-sha256</i>	aes256-sha256		
	<i>aes256-sha384</i>	aes256-sha384		
	<i>aes256-sha512</i>	aes256-sha512		
	<i>aes256gcm-prfsha1</i>	aes256gcm-prfsha1		
	<i>aes256gcm-prfsha256</i>	aes256gcm-prfsha256		
	<i>aes256gcm-prfsha384</i>	aes256gcm-prfsha384		
	<i>aes256gcm-prfsha512</i>	aes256gcm-prfsha512		
	<i>chacha20poly1305-prfsha1</i>	chacha20poly1305-prfsha1		
	<i>chacha20poly1305-prfsha256</i>	chacha20poly1305-prfsha256		
	<i>chacha20poly1305-prfsha384</i>	chacha20poly1305-prfsha384		
	<i>chacha20poly1305-prfsha512</i>	chacha20poly1305-prfsha512		
	<i>aria128-md5</i>	aria128-md5		
	<i>aria128-sha1</i>	aria128-sha1		
	<i>aria128-sha256</i>	aria128-sha256		
	<i>aria128-sha384</i>	aria128-sha384		
	<i>aria128-sha512</i>	aria128-sha512		
	<i>aria192-md5</i>	aria192-md5		
	<i>aria192-sha1</i>	aria192-sha1		
	<i>aria192-sha256</i>	aria192-sha256		

Parameter	Description	Type	Size	Default																											
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>aria192-sha384</i></td><td>aria192-sha384</td></tr><tr><td><i>aria192-sha512</i></td><td>aria192-sha512</td></tr><tr><td><i>aria256-md5</i></td><td>aria256-md5</td></tr><tr><td><i>aria256-sha1</i></td><td>aria256-sha1</td></tr><tr><td><i>aria256-sha256</i></td><td>aria256-sha256</td></tr><tr><td><i>aria256-sha384</i></td><td>aria256-sha384</td></tr><tr><td><i>aria256-sha512</i></td><td>aria256-sha512</td></tr><tr><td><i>seed-md5</i></td><td>seed-md5</td></tr><tr><td><i>seed-sha1</i></td><td>seed-sha1</td></tr><tr><td><i>seed-sha256</i></td><td>seed-sha256</td></tr><tr><td><i>seed-sha384</i></td><td>seed-sha384</td></tr><tr><td><i>seed-sha512</i></td><td>seed-sha512</td></tr></table>		Option	Description	<i>aria192-sha384</i>	aria192-sha384	<i>aria192-sha512</i>	aria192-sha512	<i>aria256-md5</i>	aria256-md5	<i>aria256-sha1</i>	aria256-sha1	<i>aria256-sha256</i>	aria256-sha256	<i>aria256-sha384</i>	aria256-sha384	<i>aria256-sha512</i>	aria256-sha512	<i>seed-md5</i>	seed-md5	<i>seed-sha1</i>	seed-sha1	<i>seed-sha256</i>	seed-sha256	<i>seed-sha384</i>	seed-sha384	<i>seed-sha512</i>	seed-sha512			
	Option	Description																													
	<i>aria192-sha384</i>	aria192-sha384																													
	<i>aria192-sha512</i>	aria192-sha512																													
	<i>aria256-md5</i>	aria256-md5																													
	<i>aria256-sha1</i>	aria256-sha1																													
	<i>aria256-sha256</i>	aria256-sha256																													
	<i>aria256-sha384</i>	aria256-sha384																													
	<i>aria256-sha512</i>	aria256-sha512																													
	<i>seed-md5</i>	seed-md5																													
	<i>seed-sha1</i>	seed-sha1																													
	<i>seed-sha256</i>	seed-sha256																													
	<i>seed-sha384</i>	seed-sha384																													
	<i>seed-sha512</i>	seed-sha512																													
psksecret	Pre-shared secret for PSK authentication (ASCII string or hexadecimal encoded with a leading 0x).	password-3	Not Specified																												
psksecret-remote	Pre-shared secret for remote side PSK authentication (ASCII string or hexadecimal encoded with a leading 0x).	password-3	Not Specified																												
reauth	Enable/disable re-authentication upon IKE SA lifetime expiration.	option	-	disable																											
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable IKE SA re-authentication.</td></tr><tr><td><i>enable</i></td><td>Enable IKE SA re-authentication.</td></tr></table>		Option	Description	<i>disable</i>	Disable IKE SA re-authentication.	<i>enable</i>	Enable IKE SA re-authentication.																							
	Option	Description																													
	<i>disable</i>	Disable IKE SA re-authentication.																													
<i>enable</i>	Enable IKE SA re-authentication.																														
rekey	Enable/disable phase1 rekey.	option	-	enable																											
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable phase1 rekey.</td></tr><tr><td><i>disable</i></td><td>Disable phase1 rekey.</td></tr></table>		Option	Description	<i>enable</i>	Enable phase1 rekey.	<i>disable</i>	Disable phase1 rekey.																							
	Option	Description																													
	<i>enable</i>	Enable phase1 rekey.																													
<i>disable</i>	Disable phase1 rekey.																														
remote-gw	Remote VPN gateway.	ipv4-address	Not Specified	0.0.0.0																											

Parameter	Description	Type	Size	Default										
remotegw-ddns	Domain name of remote gateway. For example, name.ddns.com.	string	Maximum length: 63											
rsa-signature-format	Digital Signature Authentication RSA signature format.	option	-	pkcs1										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>pkcs1</td><td>RSASSA PKCS#1 v1.5.</td></tr><tr><td>pss</td><td>RSASSA Probabilistic Signature Scheme (PSS).</td></tr></table>	Option	Description	pkcs1	RSASSA PKCS#1 v1.5.	pss	RSASSA Probabilistic Signature Scheme (PSS).							
Option	Description													
pkcs1	RSASSA PKCS#1 v1.5.													
pss	RSASSA Probabilistic Signature Scheme (PSS).													
save-password	Enable/disable saving XAuth username and password on VPN clients.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable saving XAuth username and password on VPN clients.</td></tr><tr><td>enable</td><td>Enable saving XAuth username and password on VPN clients.</td></tr></table>	Option	Description	disable	Disable saving XAuth username and password on VPN clients.	enable	Enable saving XAuth username and password on VPN clients.							
Option	Description													
disable	Disable saving XAuth username and password on VPN clients.													
enable	Enable saving XAuth username and password on VPN clients.													
send-cert-chain	Enable/disable sending certificate chain.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable sending certificate chain.</td></tr><tr><td>disable</td><td>Disable sending certificate chain.</td></tr></table>	Option	Description	enable	Enable sending certificate chain.	disable	Disable sending certificate chain.							
Option	Description													
enable	Enable sending certificate chain.													
disable	Disable sending certificate chain.													
signature-hash-alg	Digital Signature Authentication hash algorithms.	option	-	sha2-512										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>sha1</td><td>SHA1.</td></tr><tr><td>sha2-256</td><td>SHA2-256.</td></tr><tr><td>sha2-384</td><td>SHA2-384.</td></tr><tr><td>sha2-512</td><td>SHA2-512.</td></tr></table>	Option	Description	sha1	SHA1.	sha2-256	SHA2-256.	sha2-384	SHA2-384.	sha2-512	SHA2-512.			
Option	Description													
sha1	SHA1.													
sha2-256	SHA2-256.													
sha2-384	SHA2-384.													
sha2-512	SHA2-512.													
split-include-service	Split-include services.	string	Maximum length: 79											
suite-b	Use Suite-B.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Do not use UI suite.</td></tr><tr><td>suite-b-gcm-128</td><td>Use Suite-B-GCM-128.</td></tr><tr><td>suite-b-gcm-256</td><td>Use Suite-B-GCM-256.</td></tr></table>	Option	Description	disable	Do not use UI suite.	suite-b-gcm-128	Use Suite-B-GCM-128.	suite-b-gcm-256	Use Suite-B-GCM-256.					
Option	Description													
disable	Do not use UI suite.													
suite-b-gcm-128	Use Suite-B-GCM-128.													
suite-b-gcm-256	Use Suite-B-GCM-256.													

Parameter	Description	Type	Size	Default																												
type	Remote gateway type.	option	-	static																												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>static</td><td>Remote VPN gateway has fixed IP address.</td></tr><tr><td>dynamic</td><td>Remote VPN gateway has dynamic IP address.</td></tr><tr><td>ddns</td><td>Remote VPN gateway has dynamic IP address and is a dynamic DNS client.</td></tr></table>	Option	Description	static	Remote VPN gateway has fixed IP address.	dynamic	Remote VPN gateway has dynamic IP address.	ddns	Remote VPN gateway has dynamic IP address and is a dynamic DNS client.																							
Option	Description																															
static	Remote VPN gateway has fixed IP address.																															
dynamic	Remote VPN gateway has dynamic IP address.																															
ddns	Remote VPN gateway has dynamic IP address and is a dynamic DNS client.																															
unity-support	Enable/disable support for Cisco UNITY Configuration Method extensions.	option	-	enable																												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable Cisco Unity Configuration Method Extensions.</td></tr><tr><td>enable</td><td>Enable Cisco Unity Configuration Method Extensions.</td></tr></table>	Option	Description	disable	Disable Cisco Unity Configuration Method Extensions.	enable	Enable Cisco Unity Configuration Method Extensions.																									
Option	Description																															
disable	Disable Cisco Unity Configuration Method Extensions.																															
enable	Enable Cisco Unity Configuration Method Extensions.																															
usrgrp	User group name for dialup peers.	string	Maximum length: 35																													
wizard-type	GUI VPN Wizard Type.	option	-	custom																												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>custom</td><td>Custom VPN configuration.</td></tr><tr><td>dialup-forticlient</td><td>Dial Up - FortiClient Windows, Mac and Android.</td></tr><tr><td>dialup-ios</td><td>Dial Up - iPhone / iPad Native IPsec Client.</td></tr><tr><td>dialup-android</td><td>Dial Up - Android Native IPsec Client.</td></tr><tr><td>dialup-windows</td><td>Dial Up - Windows Native IPsec Client.</td></tr><tr><td>dialup-cisco</td><td>Dial Up - Cisco IPsec Client.</td></tr><tr><td>static-fortigate</td><td>Site to Site - FortiGate.</td></tr><tr><td>dialup-fortigate</td><td>Dial Up - FortiGate.</td></tr><tr><td>static-cisco</td><td>Site to Site - Cisco.</td></tr><tr><td>dialup-cisco-fw</td><td>Dialup Up - Cisco Firewall.</td></tr><tr><td>simplified-static-fortigate</td><td>Site to Site - FortiGate (SD-WAN).</td></tr><tr><td>hub-fortigate-auto-discovery</td><td>Hub role in a Hub-and-Spoke auto-discovery VPN.</td></tr><tr><td>spoke-fortigate-auto-discovery</td><td>Spoke role in a Hub-and-Spoke auto-discovery VPN.</td></tr></table>	Option	Description	custom	Custom VPN configuration.	dialup-forticlient	Dial Up - FortiClient Windows, Mac and Android.	dialup-ios	Dial Up - iPhone / iPad Native IPsec Client.	dialup-android	Dial Up - Android Native IPsec Client.	dialup-windows	Dial Up - Windows Native IPsec Client.	dialup-cisco	Dial Up - Cisco IPsec Client.	static-fortigate	Site to Site - FortiGate.	dialup-fortigate	Dial Up - FortiGate.	static-cisco	Site to Site - Cisco.	dialup-cisco-fw	Dialup Up - Cisco Firewall.	simplified-static-fortigate	Site to Site - FortiGate (SD-WAN).	hub-fortigate-auto-discovery	Hub role in a Hub-and-Spoke auto-discovery VPN.	spoke-fortigate-auto-discovery	Spoke role in a Hub-and-Spoke auto-discovery VPN.			
Option	Description																															
custom	Custom VPN configuration.																															
dialup-forticlient	Dial Up - FortiClient Windows, Mac and Android.																															
dialup-ios	Dial Up - iPhone / iPad Native IPsec Client.																															
dialup-android	Dial Up - Android Native IPsec Client.																															
dialup-windows	Dial Up - Windows Native IPsec Client.																															
dialup-cisco	Dial Up - Cisco IPsec Client.																															
static-fortigate	Site to Site - FortiGate.																															
dialup-fortigate	Dial Up - FortiGate.																															
static-cisco	Site to Site - Cisco.																															
dialup-cisco-fw	Dialup Up - Cisco Firewall.																															
simplified-static-fortigate	Site to Site - FortiGate (SD-WAN).																															
hub-fortigate-auto-discovery	Hub role in a Hub-and-Spoke auto-discovery VPN.																															
spoke-fortigate-auto-discovery	Spoke role in a Hub-and-Spoke auto-discovery VPN.																															



Parameter	Description	Type	Size	Default
xauthtype	XAuth type.	option	-	disable
	Option	Description		
	<i>disable</i>	Disable.		
	<i>client</i>	Enable as client.		
	<i>pap</i>	Enable as server PAP.		
	<i>chap</i>	Enable as server CHAP.		
	<i>auto</i>	Enable as server auto.		

\* This parameter may not exist in some models.

### config ipv4-exclude-range

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
start-ip	Start of IPv4 exclusive range.	ipv4-address	Not Specified	0.0.0.0
end-ip	End of IPv4 exclusive range.	ipv4-address	Not Specified	0.0.0.0

### config ipv6-exclude-range

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
start-ip	Start of IPv6 exclusive range.	ipv6-address	Not Specified	::
end-ip	End of IPv6 exclusive range.	ipv6-address	Not Specified	::

## config vpn ipsec phase2-interface

Configure VPN autokey tunnel.

```

config vpn ipsec phase2-interface
  Description: Configure VPN autokey tunnel.
  edit <name>
    set add-route [phase1|enable|...]
    set auto-discovery-forwarder [phase1|enable|...]
    set auto-discovery-sender [phase1|enable|...]
    set auto-negotiate [enable|disable]
    set comments {var-string}
    set dhcp-ipsec [enable|disable]
    set dhgrp {option1}, {option2}, ...
    set diffserv [enable|disable]
    set diffservcode {user}
    set dst-addr-type [subnet|range|...]
    set dst-end-ip {ipv4-address-any}
    set dst-end-ip6 {ipv6-address}
    set dst-name {string}
    set dst-name6 {string}
    set dst-port {integer}
    set dst-start-ip {ipv4-address-any}
    set dst-start-ip6 {ipv6-address}
    set dst-subnet {ipv4-classnet-any}
    set dst-subnet6 {ipv6-prefix}
    set encapsulation [tunnel-mode|transport-mode]
    set inbound-dscp-copy [phase1|enable|...]
    set initiator-ts-narrow [enable|disable]
    set ipv4-df [enable|disable]
    set keepalive [enable|disable]
    set keylife-type [seconds|kbs|...]
    set keylifekbs {integer}
    set keylifeseconds {integer}
    set l2tp [enable|disable]
    set pfs [enable|disable]
    set phase1name {string}
    set proposal {option1}, {option2}, ...
    set protocol {integer}
    set replay [enable|disable]
    set route-overlap [use-old|use-new|...]
    set single-source [enable|disable]
    set src-addr-type [subnet|range|...]
    set src-end-ip {ipv4-address-any}
    set src-end-ip6 {ipv6-address}
    set src-name {string}
    set src-name6 {string}
    set src-port {integer}
    set src-start-ip {ipv4-address-any}
    set src-start-ip6 {ipv6-address}
    set src-subnet {ipv4-classnet-any}
    set src-subnet6 {ipv6-prefix}
  next
end

```

## config vpn ipsec phase2-interface

Parameter	Description	Type	Size	Default								
add-route	Enable/disable automatic route addition.	option	-	phase1								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>phase1</i></td><td>Add route according to phase1 add-route setting.</td></tr><tr><td><i>enable</i></td><td>Add route for remote proxy ID.</td></tr><tr><td><i>disable</i></td><td>Do not add route for remote proxy ID.</td></tr></table>	Option	Description	<i>phase1</i>	Add route according to phase1 add-route setting.	<i>enable</i>	Add route for remote proxy ID.	<i>disable</i>	Do not add route for remote proxy ID.			
Option	Description											
<i>phase1</i>	Add route according to phase1 add-route setting.											
<i>enable</i>	Add route for remote proxy ID.											
<i>disable</i>	Do not add route for remote proxy ID.											
auto-discovery-forwarder	Enable/disable forwarding short-cut messages.	option	-	phase1								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>phase1</i></td><td>Forward short-cut messages according to the phase1 auto-discovery-forwarder setting.</td></tr><tr><td><i>enable</i></td><td>Enable forwarding auto-discovery short-cut messages.</td></tr><tr><td><i>disable</i></td><td>Disable forwarding auto-discovery short-cut messages.</td></tr></table>	Option	Description	<i>phase1</i>	Forward short-cut messages according to the phase1 auto-discovery-forwarder setting.	<i>enable</i>	Enable forwarding auto-discovery short-cut messages.	<i>disable</i>	Disable forwarding auto-discovery short-cut messages.			
Option	Description											
<i>phase1</i>	Forward short-cut messages according to the phase1 auto-discovery-forwarder setting.											
<i>enable</i>	Enable forwarding auto-discovery short-cut messages.											
<i>disable</i>	Disable forwarding auto-discovery short-cut messages.											
auto-discovery-sender	Enable/disable sending short-cut messages.	option	-	phase1								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>phase1</i></td><td>Send short-cut messages according to the phase1 auto-discovery-sender setting.</td></tr><tr><td><i>enable</i></td><td>Enable sending auto-discovery short-cut messages.</td></tr><tr><td><i>disable</i></td><td>Disable sending auto-discovery short-cut messages.</td></tr></table>	Option	Description	<i>phase1</i>	Send short-cut messages according to the phase1 auto-discovery-sender setting.	<i>enable</i>	Enable sending auto-discovery short-cut messages.	<i>disable</i>	Disable sending auto-discovery short-cut messages.			
Option	Description											
<i>phase1</i>	Send short-cut messages according to the phase1 auto-discovery-sender setting.											
<i>enable</i>	Enable sending auto-discovery short-cut messages.											
<i>disable</i>	Disable sending auto-discovery short-cut messages.											
auto-negotiate	Enable/disable IPsec SA auto-negotiation.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											
comments	Comment.	var-string	Maximum length: 255									
dhcp-ipsec	Enable/disable DHCP-IPsec.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
Option	Description											
<i>enable</i>	Enable setting.											
<i>disable</i>	Disable setting.											

Parameter	Description	Type	Size	Default																																				
dhgrp	Phase2 DH group.	option	-	14																																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>1</td><td>DH Group 1.</td></tr><tr><td>2</td><td>DH Group 2.</td></tr><tr><td>5</td><td>DH Group 5.</td></tr><tr><td>14</td><td>DH Group 14.</td></tr><tr><td>15</td><td>DH Group 15.</td></tr><tr><td>16</td><td>DH Group 16.</td></tr><tr><td>17</td><td>DH Group 17.</td></tr><tr><td>18</td><td>DH Group 18.</td></tr><tr><td>19</td><td>DH Group 19.</td></tr><tr><td>20</td><td>DH Group 20.</td></tr><tr><td>21</td><td>DH Group 21.</td></tr><tr><td>27</td><td>DH Group 27.</td></tr><tr><td>28</td><td>DH Group 28.</td></tr><tr><td>29</td><td>DH Group 29.</td></tr><tr><td>30</td><td>DH Group 30.</td></tr><tr><td>31</td><td>DH Group 31.</td></tr><tr><td>32</td><td>DH Group 32.</td></tr></table>	Option	Description	1	DH Group 1.	2	DH Group 2.	5	DH Group 5.	14	DH Group 14.	15	DH Group 15.	16	DH Group 16.	17	DH Group 17.	18	DH Group 18.	19	DH Group 19.	20	DH Group 20.	21	DH Group 21.	27	DH Group 27.	28	DH Group 28.	29	DH Group 29.	30	DH Group 30.	31	DH Group 31.	32	DH Group 32.			
	Option	Description																																						
	1	DH Group 1.																																						
	2	DH Group 2.																																						
	5	DH Group 5.																																						
	14	DH Group 14.																																						
	15	DH Group 15.																																						
	16	DH Group 16.																																						
	17	DH Group 17.																																						
	18	DH Group 18.																																						
	19	DH Group 19.																																						
	20	DH Group 20.																																						
	21	DH Group 21.																																						
	27	DH Group 27.																																						
	28	DH Group 28.																																						
	29	DH Group 29.																																						
	30	DH Group 30.																																						
	31	DH Group 31.																																						
32	DH Group 32.																																							
diffserv	Enable/disable applying DSCP value to the IPsec tunnel outer IP header.	option	-	disable																																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>	Option	Description	enable	Enable setting.	disable	Disable setting.																																	
	Option	Description																																						
	enable	Enable setting.																																						
disable	Disable setting.																																							
diffservcode	DSCP value to be applied to the IPsec tunnel outer IP header.	user	Not Specified																																					
dst-addr-type	Remote proxy ID type.	option	-	subnet																																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>subnet</td><td>IPv4 subnet.</td></tr></table>	Option	Description	subnet	IPv4 subnet.																																			
	Option	Description																																						
subnet	IPv4 subnet.																																							

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>range</i>	IPv4 range.		
	<i>ip</i>	IPv4 IP.		
	<i>name</i>	IPv4 firewall address or group name.		
	<i>subnet6</i>	IPv6 subnet.		
	<i>range6</i>	IPv6 range.		
	<i>ip6</i>	IPv6 IP.		
	<i>name6</i>	IPv6 firewall address or group name.		
dst-end-ip	Remote proxy ID IPv4 end.	ipv4-address-any	Not Specified	0.0.0.0
dst-end-ip6	Remote proxy ID IPv6 end.	ipv6-address	Not Specified	::
dst-name	Remote proxy ID name.	string	Maximum length: 79	
dst-name6	Remote proxy ID name.	string	Maximum length: 79	
dst-port	Quick mode destination port.	integer	Minimum value: 0 Maximum value: 65535	0
dst-start-ip	Remote proxy ID IPv4 start.	ipv4-address-any	Not Specified	0.0.0.0
dst-start-ip6	Remote proxy ID IPv6 start.	ipv6-address	Not Specified	::
dst-subnet	Remote proxy ID IPv4 subnet.	ipv4-classnet-any	Not Specified	0.0.0.0 0.0.0.0
dst-subnet6	Remote proxy ID IPv6 subnet.	ipv6-prefix	Not Specified	::/0
encapsulation	ESP encapsulation mode.	option	-	tunnel-mode
	<b>Option</b>	<b>Description</b>		
	<i>tunnel-mode</i>	Use tunnel mode encapsulation.		
	<i>transport-mode</i>	Use transport mode encapsulation.		
inbound-dscp-copy	Enable/disable copying of the DSCP values in the ESP header to the inner IP Header.	option	-	phase1

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>phase1</i></td><td>copy the dscp in the ESP header to the inner IP Header according to the phase1 inbound_dscp_copy setting.</td></tr><tr><td><i>enable</i></td><td>Enable copying of the DSCP values in the ESP header to the inner IP Header.</td></tr><tr><td><i>disable</i></td><td>Disable copying of the DSCP values in the ESP header to the inner IP Header.</td></tr></table>	Option	Description	<i>phase1</i>	copy the dscp in the ESP header to the inner IP Header according to the phase1 inbound_dscp_copy setting.	<i>enable</i>	Enable copying of the DSCP values in the ESP header to the inner IP Header.	<i>disable</i>	Disable copying of the DSCP values in the ESP header to the inner IP Header.			
	Option	Description										
	<i>phase1</i>	copy the dscp in the ESP header to the inner IP Header according to the phase1 inbound_dscp_copy setting.										
	<i>enable</i>	Enable copying of the DSCP values in the ESP header to the inner IP Header.										
<i>disable</i>	Disable copying of the DSCP values in the ESP header to the inner IP Header.											
initiator-ts-narrow	Enable/disable traffic selector narrowing for IKEv2 initiator.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
	Option	Description										
	<i>enable</i>	Enable setting.										
<i>disable</i>	Disable setting.											
ipv4-df	Enable/disable setting and resetting of IPv4 'Don't Fragment' bit.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Set IPv4 DF the same as original packet.</td></tr><tr><td><i>disable</i></td><td>Reset IPv4 DF.</td></tr></table>	Option	Description	<i>enable</i>	Set IPv4 DF the same as original packet.	<i>disable</i>	Reset IPv4 DF.					
	Option	Description										
	<i>enable</i>	Set IPv4 DF the same as original packet.										
<i>disable</i>	Reset IPv4 DF.											
keepalive	Enable/disable keep alive.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
	Option	Description										
	<i>enable</i>	Enable setting.										
<i>disable</i>	Disable setting.											
keylife-type	Keylife type.	option	-	seconds								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>seconds</i></td><td>Key life in seconds.</td></tr><tr><td><i>kbs</i></td><td>Key life in kilobytes.</td></tr><tr><td><i>both</i></td><td>Key life both.</td></tr></table>	Option	Description	<i>seconds</i>	Key life in seconds.	<i>kbs</i>	Key life in kilobytes.	<i>both</i>	Key life both.			
	Option	Description										
	<i>seconds</i>	Key life in seconds.										
	<i>kbs</i>	Key life in kilobytes.										
<i>both</i>	Key life both.											
keylifekbs	Phase2 key life in number of kilobytes of traffic.	integer	Minimum value: 5120 Maximum value: 4294967295	5120								

Parameter	Description	Type	Size	Default
keylifeseconds	Phase2 key life in time in seconds.	integer	Minimum value: 120 Maximum value: 172800	43200
l2tp	Enable/disable L2TP over IPsec.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable L2TP over IPsec.		
	<i>disable</i>	Disable L2TP over IPsec.		
name	IPsec tunnel name.	string	Maximum length: 35	
pfs	Enable/disable PFS feature.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
phase1name	Phase 1 determines the options required for phase 2.	string	Maximum length: 15	
proposal	Phase2 proposal.	option	-	
	<b>Option</b>	<b>Description</b>		
	<i>null-md5</i>	null-md5		
	<i>null-sha1</i>	null-sha1		
	<i>null-sha256</i>	null-sha256		
	<i>null-sha384</i>	null-sha384		
	<i>null-sha512</i>	null-sha512		
	<i>des-null</i>	des-null		
	<i>des-md5</i>	des-md5		
	<i>des-sha1</i>	des-sha1		
	<i>des-sha256</i>	des-sha256		
	<i>des-sha384</i>	des-sha384		
	<i>des-sha512</i>	des-sha512		
	<i>3des-null</i>	3des-null		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>3des-md5</i>	3des-md5		
	<i>3des-sha1</i>	3des-sha1		
	<i>3des-sha256</i>	3des-sha256		
	<i>3des-sha384</i>	3des-sha384		
	<i>3des-sha512</i>	3des-sha512		
	<i>aes128-null</i>	aes128-null		
	<i>aes128-md5</i>	aes128-md5		
	<i>aes128-sha1</i>	aes128-sha1		
	<i>aes128-sha256</i>	aes128-sha256		
	<i>aes128-sha384</i>	aes128-sha384		
	<i>aes128-sha512</i>	aes128-sha512		
	<i>aes128gcm</i>	aes128gcm		
	<i>aes192-null</i>	aes192-null		
	<i>aes192-md5</i>	aes192-md5		
	<i>aes192-sha1</i>	aes192-sha1		
	<i>aes192-sha256</i>	aes192-sha256		
	<i>aes192-sha384</i>	aes192-sha384		
	<i>aes192-sha512</i>	aes192-sha512		
	<i>aes256-null</i>	aes256-null		
	<i>aes256-md5</i>	aes256-md5		
	<i>aes256-sha1</i>	aes256-sha1		
	<i>aes256-sha256</i>	aes256-sha256		
	<i>aes256-sha384</i>	aes256-sha384		
	<i>aes256-sha512</i>	aes256-sha512		
	<i>aes256gcm</i>	aes256gcm		
	<i>chacha20poly1305</i>	chacha20poly1305		
	<i>aria128-null</i>	aria128-null		
	<i>aria128-md5</i>	aria128-md5		
	<i>aria128-sha1</i>	aria128-sha1		



Parameter	Description	Type	Size	Default																																												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>aria128-sha256</i></td><td>aria128-sha256</td></tr><tr><td><i>aria128-sha384</i></td><td>aria128-sha384</td></tr><tr><td><i>aria128-sha512</i></td><td>aria128-sha512</td></tr><tr><td><i>aria192-null</i></td><td>aria192-null</td></tr><tr><td><i>aria192-md5</i></td><td>aria192-md5</td></tr><tr><td><i>aria192-sha1</i></td><td>aria192-sha1</td></tr><tr><td><i>aria192-sha256</i></td><td>aria192-sha256</td></tr><tr><td><i>aria192-sha384</i></td><td>aria192-sha384</td></tr><tr><td><i>aria192-sha512</i></td><td>aria192-sha512</td></tr><tr><td><i>aria256-null</i></td><td>aria256-null</td></tr><tr><td><i>aria256-md5</i></td><td>aria256-md5</td></tr><tr><td><i>aria256-sha1</i></td><td>aria256-sha1</td></tr><tr><td><i>aria256-sha256</i></td><td>aria256-sha256</td></tr><tr><td><i>aria256-sha384</i></td><td>aria256-sha384</td></tr><tr><td><i>aria256-sha512</i></td><td>aria256-sha512</td></tr><tr><td><i>seed-null</i></td><td>seed-null</td></tr><tr><td><i>seed-md5</i></td><td>seed-md5</td></tr><tr><td><i>seed-sha1</i></td><td>seed-sha1</td></tr><tr><td><i>seed-sha256</i></td><td>seed-sha256</td></tr><tr><td><i>seed-sha384</i></td><td>seed-sha384</td></tr><tr><td><i>seed-sha512</i></td><td>seed-sha512</td></tr></table>	Option	Description	<i>aria128-sha256</i>	aria128-sha256	<i>aria128-sha384</i>	aria128-sha384	<i>aria128-sha512</i>	aria128-sha512	<i>aria192-null</i>	aria192-null	<i>aria192-md5</i>	aria192-md5	<i>aria192-sha1</i>	aria192-sha1	<i>aria192-sha256</i>	aria192-sha256	<i>aria192-sha384</i>	aria192-sha384	<i>aria192-sha512</i>	aria192-sha512	<i>aria256-null</i>	aria256-null	<i>aria256-md5</i>	aria256-md5	<i>aria256-sha1</i>	aria256-sha1	<i>aria256-sha256</i>	aria256-sha256	<i>aria256-sha384</i>	aria256-sha384	<i>aria256-sha512</i>	aria256-sha512	<i>seed-null</i>	seed-null	<i>seed-md5</i>	seed-md5	<i>seed-sha1</i>	seed-sha1	<i>seed-sha256</i>	seed-sha256	<i>seed-sha384</i>	seed-sha384	<i>seed-sha512</i>	seed-sha512			
	Option	Description																																														
	<i>aria128-sha256</i>	aria128-sha256																																														
	<i>aria128-sha384</i>	aria128-sha384																																														
	<i>aria128-sha512</i>	aria128-sha512																																														
	<i>aria192-null</i>	aria192-null																																														
	<i>aria192-md5</i>	aria192-md5																																														
	<i>aria192-sha1</i>	aria192-sha1																																														
	<i>aria192-sha256</i>	aria192-sha256																																														
	<i>aria192-sha384</i>	aria192-sha384																																														
	<i>aria192-sha512</i>	aria192-sha512																																														
	<i>aria256-null</i>	aria256-null																																														
	<i>aria256-md5</i>	aria256-md5																																														
	<i>aria256-sha1</i>	aria256-sha1																																														
	<i>aria256-sha256</i>	aria256-sha256																																														
	<i>aria256-sha384</i>	aria256-sha384																																														
	<i>aria256-sha512</i>	aria256-sha512																																														
	<i>seed-null</i>	seed-null																																														
	<i>seed-md5</i>	seed-md5																																														
	<i>seed-sha1</i>	seed-sha1																																														
	<i>seed-sha256</i>	seed-sha256																																														
	<i>seed-sha384</i>	seed-sha384																																														
	<i>seed-sha512</i>	seed-sha512																																														
protocol	Quick mode protocol selector.	integer	Minimum value: 0 Maximum value: 255	0																																												
replay	Enable/disable replay detection.	option	-	enable																																												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.																																									
	Option	Description																																														
	<i>enable</i>	Enable setting.																																														
<i>disable</i>	Disable setting.																																															

Parameter	Description	Type	Size	Default
route-overlap	Action for overlapping routes.	option	-	use-new
	<b>Option</b>	<b>Description</b>		
	<i>use-old</i>	Use the old route and do not add the new route.		
	<i>use-new</i>	Delete the old route and add the new route.		
	<i>allow</i>	Allow overlapping routes.		
single-source	Enable/disable single source IP restriction.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Only single source IP will be accepted.		
	<i>disable</i>	Source IP range will be accepted.		
src-addr-type	Local proxy ID type.	option	-	subnet
	<b>Option</b>	<b>Description</b>		
	<i>subnet</i>	IPv4 subnet.		
	<i>range</i>	IPv4 range.		
	<i>ip</i>	IPv4 IP.		
	<i>name</i>	IPv4 firewall address or group name.		
	<i>subnet6</i>	IPv6 subnet.		
	<i>range6</i>	IPv6 range.		
	<i>ip6</i>	IPv6 IP.		
	<i>name6</i>	IPv6 firewall address or group name.		
src-end-ip	Local proxy ID end.	ipv4-address-any	Not Specified	0.0.0.0
src-end-ip6	Local proxy ID IPv6 end.	ipv6-address	Not Specified	::
src-name	Local proxy ID name.	string	Maximum length: 79	
src-name6	Local proxy ID name.	string	Maximum length: 79	
src-port	Quick mode source port.	integer	Minimum value: 0 Maximum value: 65535	0

Parameter	Description	Type	Size	Default
src-start-ip	Local proxy ID start.	ipv4-address-any	Not Specified	0.0.0.0
src-start-ip6	Local proxy ID IPv6 start.	ipv6-address	Not Specified	::
src-subnet	Local proxy ID subnet.	ipv4-classnet-any	Not Specified	0.0.0.0 0.0.0.0
src-subnet6	Local proxy ID IPv6 subnet.	ipv6-prefix	Not Specified	::/0

## config vpn ipsec phase2

Configure VPN autokey tunnel.

```
config vpn ipsec phase2
    Description: Configure VPN autokey tunnel.
    edit <name>
        set add-route [phase1|enable|...]
        set auto-negotiate [enable|disable]
        set comments {var-string}
        set dhcp-ipsec [enable|disable]
        set dhgrp {option1}, {option2}, ...
        set diffserv [enable|disable]
        set diffservcode {user}
        set dst-addr-type [subnet|range|...]
        set dst-end-ip {ipv4-address-any}
        set dst-end-ip6 {ipv6-address}
        set dst-name {string}
        set dst-name6 {string}
        set dst-port {integer}
        set dst-start-ip {ipv4-address-any}
        set dst-start-ip6 {ipv6-address}
        set dst-subnet {ipv4-classnet-any}
        set dst-subnet6 {ipv6-prefix}
        set encapsulation [tunnel-mode|transport-mode]
        set inbound-dscp-copy [phase1|enable|...]
        set initiator-ts-narrow [enable|disable]
        set ipv4-df [enable|disable]
        set keepalive [enable|disable]
        set keylife-type [seconds|kbs|...]
        set keylifekbs {integer}
        set keylifeseconds {integer}
        set l2tp [enable|disable]
        set pfs [enable|disable]
        set phase1name {string}
        set proposal {option1}, {option2}, ...
        set protocol {integer}
        set replay [enable|disable]
        set route-overlap [use-old|use-new|...]
        set selector-match [exact|subset|...]
        set single-source [enable|disable]
        set src-addr-type [subnet|range|...]
```

```

set src-end-ip {ipv4-address-any}
set src-end-ip6 {ipv6-address}
set src-name {string}
set src-name6 {string}
set src-port {integer}
set src-start-ip {ipv4-address-any}
set src-start-ip6 {ipv6-address}
set src-subnet {ipv4-classnet-any}
set src-subnet6 {ipv6-prefix}
set use-natip [enable|disable]
next
end

```

## config vpn ipsec phase2

Parameter	Description	Type	Size	Default
add-route	Enable/disable automatic route addition.	option	-	phase1
	Option	Description		
	phase1	Add route according to phase1 add-route setting.		
	enable	Add route for remote proxy ID.		
	disable	Do not add route for remote proxy ID.		
auto-negotiate	Enable/disable IPsec SA auto-negotiation.	option	-	disable
	Option	Description		
	enable	Enable setting.		
	disable	Disable setting.		
comments	Comment.	var-string	Maximum length: 255	
dhcp-ipsec	Enable/disable DHCP-IPsec.	option	-	disable
	Option	Description		
	enable	Enable setting.		
	disable	Disable setting.		
dhgrp	Phase2 DH group.	option	-	14
	Option	Description		
	1	DH Group 1.		
	2	DH Group 2.		
	5	DH Group 5.		

Parameter	Description	Type	Size	Default																														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>14</td><td>DH Group 14.</td></tr><tr><td>15</td><td>DH Group 15.</td></tr><tr><td>16</td><td>DH Group 16.</td></tr><tr><td>17</td><td>DH Group 17.</td></tr><tr><td>18</td><td>DH Group 18.</td></tr><tr><td>19</td><td>DH Group 19.</td></tr><tr><td>20</td><td>DH Group 20.</td></tr><tr><td>21</td><td>DH Group 21.</td></tr><tr><td>27</td><td>DH Group 27.</td></tr><tr><td>28</td><td>DH Group 28.</td></tr><tr><td>29</td><td>DH Group 29.</td></tr><tr><td>30</td><td>DH Group 30.</td></tr><tr><td>31</td><td>DH Group 31.</td></tr><tr><td>32</td><td>DH Group 32.</td></tr></table>	Option	Description	14	DH Group 14.	15	DH Group 15.	16	DH Group 16.	17	DH Group 17.	18	DH Group 18.	19	DH Group 19.	20	DH Group 20.	21	DH Group 21.	27	DH Group 27.	28	DH Group 28.	29	DH Group 29.	30	DH Group 30.	31	DH Group 31.	32	DH Group 32.			
	Option	Description																																
	14	DH Group 14.																																
	15	DH Group 15.																																
	16	DH Group 16.																																
	17	DH Group 17.																																
	18	DH Group 18.																																
	19	DH Group 19.																																
	20	DH Group 20.																																
	21	DH Group 21.																																
	27	DH Group 27.																																
	28	DH Group 28.																																
	29	DH Group 29.																																
	30	DH Group 30.																																
	31	DH Group 31.																																
	32	DH Group 32.																																
diffserv	Enable/disable applying DSCP value to the IPsec tunnel outer IP header.	option	-	disable																														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>	Option	Description	enable	Enable setting.	disable	Disable setting.																											
	Option	Description																																
	enable	Enable setting.																																
disable	Disable setting.																																	
diffservcode	DSCP value to be applied to the IPsec tunnel outer IP header.	user	Not Specified																															
dst-addr-type	Remote proxy ID type.	option	-	subnet																														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>subnet</td><td>IPv4 subnet.</td></tr><tr><td>range</td><td>IPv4 range.</td></tr><tr><td>ip</td><td>IPv4 IP.</td></tr><tr><td>name</td><td>IPv4 firewall address or group name.</td></tr></table>	Option	Description	subnet	IPv4 subnet.	range	IPv4 range.	ip	IPv4 IP.	name	IPv4 firewall address or group name.																							
	Option	Description																																
	subnet	IPv4 subnet.																																
	range	IPv4 range.																																
	ip	IPv4 IP.																																
name	IPv4 firewall address or group name.																																	
dst-end-ip	Remote proxy ID IPv4 end.	ipv4-address-any	Not Specified	0.0.0.0																														

Parameter	Description	Type	Size	Default
dst-end-ip6	Remote proxy ID IPv6 end.	ipv6-address	Not Specified	::
dst-name	Remote proxy ID name.	string	Maximum length: 79	
dst-name6	Remote proxy ID name.	string	Maximum length: 79	
dst-port	Quick mode destination port.	integer	Minimum value: 0 Maximum value: 65535	0
dst-start-ip	Remote proxy ID IPv4 start.	ipv4-address-any	Not Specified	0.0.0.0
dst-start-ip6	Remote proxy ID IPv6 start.	ipv6-address	Not Specified	::
dst-subnet	Remote proxy ID IPv4 subnet.	ipv4-classnet-any	Not Specified	0.0.0.0 0.0.0.0
dst-subnet6	Remote proxy ID IPv6 subnet.	ipv6-prefix	Not Specified	::/0
encapsulation	ESP encapsulation mode.	option	-	tunnel-mode
	<b>Option</b> <b>Description</b>			
	<i>tunnel-mode</i>	Use tunnel mode encapsulation.		
	<i>transport-mode</i>	Use transport mode encapsulation.		
inbound-dscp-copy	Enable/disable copying of the DSCP values in the ESP header to the inner IP Header.	option	-	phase1
	<b>Option</b> <b>Description</b>			
	<i>phase1</i>	copy the dscp in the ESP header to the inner IP Header according to the phase1 inbound_dscp_copy setting.		
	<i>enable</i>	Enable copying of the DSCP values in the ESP header to the inner IP Header.		
	<i>disable</i>	Disable copying of the DSCP values in the ESP header to the inner IP Header.		
initiator-ts-narrow	Enable/disable traffic selector narrowing for IKEV2 initiator.	option	-	disable

Parameter	Description	Type	Size	Default
	Option Description			
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
ipv4-df	Enable/disable setting and resetting of IPv4 'Don't Fragment' bit.	option	-	disable
	Option Description			
	<i>enable</i>	Set IPv4 DF the same as original packet.		
	<i>disable</i>	Reset IPv4 DF.		
keepalive	Enable/disable keep alive.	option	-	disable
	Option Description			
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
keylife-type	Keylife type.	option	-	seconds
	Option Description			
	<i>seconds</i>	Key life in seconds.		
	<i>kbs</i>	Key life in kilobytes.		
	<i>both</i>	Key life both.		
keylifekbs	Phase2 key life in number of kilobytes of traffic.	integer	Minimum value: 5120 Maximum value: 4294967295	5120
keylifeseconds	Phase2 key life in time in seconds.	integer	Minimum value: 120 Maximum value: 172800	43200
l2tp	Enable/disable L2TP over IPsec.	option	-	disable
	Option Description			
	<i>enable</i>	Enable L2TP over IPsec.		
	<i>disable</i>	Disable L2TP over IPsec.		

Parameter	Description	Type	Size	Default																																										
name	IPsec tunnel name.	string	Maximum length: 35																																											
pfs	Enable/disable PFS feature.	option	-	enable																																										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>				Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.																																				
	Option	Description																																												
	<i>enable</i>	Enable setting.																																												
	<i>disable</i>	Disable setting.																																												
phase1name	Phase 1 determines the options required for phase 2.	string	Maximum length: 35																																											
proposal	Phase2 proposal.	option	-																																											
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>null-md5</i></td><td>null-md5</td></tr><tr><td><i>null-sha1</i></td><td>null-sha1</td></tr><tr><td><i>null-sha256</i></td><td>null-sha256</td></tr><tr><td><i>null-sha384</i></td><td>null-sha384</td></tr><tr><td><i>null-sha512</i></td><td>null-sha512</td></tr><tr><td><i>des-null</i></td><td>des-null</td></tr><tr><td><i>des-md5</i></td><td>des-md5</td></tr><tr><td><i>des-sha1</i></td><td>des-sha1</td></tr><tr><td><i>des-sha256</i></td><td>des-sha256</td></tr><tr><td><i>des-sha384</i></td><td>des-sha384</td></tr><tr><td><i>des-sha512</i></td><td>des-sha512</td></tr><tr><td><i>3des-null</i></td><td>3des-null</td></tr><tr><td><i>3des-md5</i></td><td>3des-md5</td></tr><tr><td><i>3des-sha1</i></td><td>3des-sha1</td></tr><tr><td><i>3des-sha256</i></td><td>3des-sha256</td></tr><tr><td><i>3des-sha384</i></td><td>3des-sha384</td></tr><tr><td><i>3des-sha512</i></td><td>3des-sha512</td></tr><tr><td><i>aes128-null</i></td><td>aes128-null</td></tr><tr><td><i>aes128-md5</i></td><td>aes128-md5</td></tr><tr><td><i>aes128-sha1</i></td><td>aes128-sha1</td></tr></table>				Option	Description	<i>null-md5</i>	null-md5	<i>null-sha1</i>	null-sha1	<i>null-sha256</i>	null-sha256	<i>null-sha384</i>	null-sha384	<i>null-sha512</i>	null-sha512	<i>des-null</i>	des-null	<i>des-md5</i>	des-md5	<i>des-sha1</i>	des-sha1	<i>des-sha256</i>	des-sha256	<i>des-sha384</i>	des-sha384	<i>des-sha512</i>	des-sha512	<i>3des-null</i>	3des-null	<i>3des-md5</i>	3des-md5	<i>3des-sha1</i>	3des-sha1	<i>3des-sha256</i>	3des-sha256	<i>3des-sha384</i>	3des-sha384	<i>3des-sha512</i>	3des-sha512	<i>aes128-null</i>	aes128-null	<i>aes128-md5</i>	aes128-md5	<i>aes128-sha1</i>	aes128-sha1
	Option	Description																																												
	<i>null-md5</i>	null-md5																																												
	<i>null-sha1</i>	null-sha1																																												
	<i>null-sha256</i>	null-sha256																																												
	<i>null-sha384</i>	null-sha384																																												
	<i>null-sha512</i>	null-sha512																																												
	<i>des-null</i>	des-null																																												
	<i>des-md5</i>	des-md5																																												
	<i>des-sha1</i>	des-sha1																																												
	<i>des-sha256</i>	des-sha256																																												
	<i>des-sha384</i>	des-sha384																																												
	<i>des-sha512</i>	des-sha512																																												
	<i>3des-null</i>	3des-null																																												
	<i>3des-md5</i>	3des-md5																																												
	<i>3des-sha1</i>	3des-sha1																																												
	<i>3des-sha256</i>	3des-sha256																																												
	<i>3des-sha384</i>	3des-sha384																																												
	<i>3des-sha512</i>	3des-sha512																																												
	<i>aes128-null</i>	aes128-null																																												
	<i>aes128-md5</i>	aes128-md5																																												
<i>aes128-sha1</i>	aes128-sha1																																													



Parameter	Description	Type	Size	Default
	Option	Description		
	<i>aes128-sha256</i>	aes128-sha256		
	<i>aes128-sha384</i>	aes128-sha384		
	<i>aes128-sha512</i>	aes128-sha512		
	<i>aes128gcm</i>	aes128gcm		
	<i>aes192-null</i>	aes192-null		
	<i>aes192-md5</i>	aes192-md5		
	<i>aes192-sha1</i>	aes192-sha1		
	<i>aes192-sha256</i>	aes192-sha256		
	<i>aes192-sha384</i>	aes192-sha384		
	<i>aes192-sha512</i>	aes192-sha512		
	<i>aes256-null</i>	aes256-null		
	<i>aes256-md5</i>	aes256-md5		
	<i>aes256-sha1</i>	aes256-sha1		
	<i>aes256-sha256</i>	aes256-sha256		
	<i>aes256-sha384</i>	aes256-sha384		
	<i>aes256-sha512</i>	aes256-sha512		
	<i>aes256gcm</i>	aes256gcm		
	<i>chacha20poly1305</i>	chacha20poly1305		
	<i>aria128-null</i>	aria128-null		
	<i>aria128-md5</i>	aria128-md5		
	<i>aria128-sha1</i>	aria128-sha1		
	<i>aria128-sha256</i>	aria128-sha256		
	<i>aria128-sha384</i>	aria128-sha384		
	<i>aria128-sha512</i>	aria128-sha512		
	<i>aria192-null</i>	aria192-null		
	<i>aria192-md5</i>	aria192-md5		
	<i>aria192-sha1</i>	aria192-sha1		
	<i>aria192-sha256</i>	aria192-sha256		
	<i>aria192-sha384</i>	aria192-sha384		

Parameter	Description	Type	Size	Default																												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>aria192-sha512</i></td><td>aria192-sha512</td></tr><tr><td><i>aria256-null</i></td><td>aria256-null</td></tr><tr><td><i>aria256-md5</i></td><td>aria256-md5</td></tr><tr><td><i>aria256-sha1</i></td><td>aria256-sha1</td></tr><tr><td><i>aria256-sha256</i></td><td>aria256-sha256</td></tr><tr><td><i>aria256-sha384</i></td><td>aria256-sha384</td></tr><tr><td><i>aria256-sha512</i></td><td>aria256-sha512</td></tr><tr><td><i>seed-null</i></td><td>seed-null</td></tr><tr><td><i>seed-md5</i></td><td>seed-md5</td></tr><tr><td><i>seed-sha1</i></td><td>seed-sha1</td></tr><tr><td><i>seed-sha256</i></td><td>seed-sha256</td></tr><tr><td><i>seed-sha384</i></td><td>seed-sha384</td></tr><tr><td><i>seed-sha512</i></td><td>seed-sha512</td></tr></table>	Option	Description	<i>aria192-sha512</i>	aria192-sha512	<i>aria256-null</i>	aria256-null	<i>aria256-md5</i>	aria256-md5	<i>aria256-sha1</i>	aria256-sha1	<i>aria256-sha256</i>	aria256-sha256	<i>aria256-sha384</i>	aria256-sha384	<i>aria256-sha512</i>	aria256-sha512	<i>seed-null</i>	seed-null	<i>seed-md5</i>	seed-md5	<i>seed-sha1</i>	seed-sha1	<i>seed-sha256</i>	seed-sha256	<i>seed-sha384</i>	seed-sha384	<i>seed-sha512</i>	seed-sha512			
	Option	Description																														
	<i>aria192-sha512</i>	aria192-sha512																														
	<i>aria256-null</i>	aria256-null																														
	<i>aria256-md5</i>	aria256-md5																														
	<i>aria256-sha1</i>	aria256-sha1																														
	<i>aria256-sha256</i>	aria256-sha256																														
	<i>aria256-sha384</i>	aria256-sha384																														
	<i>aria256-sha512</i>	aria256-sha512																														
	<i>seed-null</i>	seed-null																														
	<i>seed-md5</i>	seed-md5																														
	<i>seed-sha1</i>	seed-sha1																														
	<i>seed-sha256</i>	seed-sha256																														
	<i>seed-sha384</i>	seed-sha384																														
	<i>seed-sha512</i>	seed-sha512																														
protocol	Quick mode protocol selector.	integer	Minimum value: 0 Maximum value: 255	0																												
replay	Enable/disable replay detection.	option	-	enable																												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.																									
	Option	Description																														
	<i>enable</i>	Enable setting.																														
<i>disable</i>	Disable setting.																															
route-overlap	Action for overlapping routes.	option	-	use-new																												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>use-old</i></td><td>Use the old route and do not add the new route.</td></tr><tr><td><i>use-new</i></td><td>Delete the old route and add the new route.</td></tr><tr><td><i>allow</i></td><td>Allow overlapping routes.</td></tr></table>	Option	Description	<i>use-old</i>	Use the old route and do not add the new route.	<i>use-new</i>	Delete the old route and add the new route.	<i>allow</i>	Allow overlapping routes.																							
	Option	Description																														
	<i>use-old</i>	Use the old route and do not add the new route.																														
	<i>use-new</i>	Delete the old route and add the new route.																														
<i>allow</i>	Allow overlapping routes.																															
selector-match	Match type to use when comparing selectors.	option	-	auto																												

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>exact</i>	Match selectors exactly.		
	<i>subset</i>	Match selectors by subset.		
	<i>auto</i>	Use subset or exact match depending on selector address type.		
single-source	Enable/disable single source IP restriction.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Only single source IP will be accepted.		
	<i>disable</i>	Source IP range will be accepted.		
src-addr-type	Local proxy ID type.	option	-	subnet
	<b>Option</b>	<b>Description</b>		
	<i>subnet</i>	IPv4 subnet.		
	<i>range</i>	IPv4 range.		
	<i>ip</i>	IPv4 IP.		
	<i>name</i>	IPv4 firewall address or group name.		
src-end-ip	Local proxy ID end.	ipv4-address-any	Not Specified	0.0.0.0
src-end-ip6	Local proxy ID IPv6 end.	ipv6-address	Not Specified	::
src-name	Local proxy ID name.	string	Maximum length: 79	
src-name6	Local proxy ID name.	string	Maximum length: 79	
src-port	Quick mode source port.	integer	Minimum value: 0 Maximum value: 65535	0
src-start-ip	Local proxy ID start.	ipv4-address-any	Not Specified	0.0.0.0
src-start-ip6	Local proxy ID IPv6 start.	ipv6-address	Not Specified	::
src-subnet	Local proxy ID subnet.	ipv4-classnet-any	Not Specified	0.0.0.0 0.0.0.0

Parameter	Description	Type	Size	Default
src-subnet6	Local proxy ID IPv6 subnet.	ipv6-prefix	Not Specified	::/0
use-natip	Enable to use the FortiGate public IP as the source selector when outbound NAT is used.	option	-	enable
	Option	Description		
	<i>enable</i>	Replace source selector with interface IP when using outbound NAT.		
	<i>disable</i>	Do not modify source selector when using outbound NAT.		

## config vpn l2tp

Configure L2TP.

```
config vpn l2tp
    Description: Configure L2TP.
    set compress [enable|disable]
    set eip {ipv4-address}
    set enforce-ipsec [enable|disable]
    set hello-interval {integer}
    set lcp-echo-interval {integer}
    set lcp-max-echo-fails {integer}
    set sip {ipv4-address}
    set status [enable|disable]
    set usrgrp {string}
end
```

## config vpn l2tp

Parameter	Description	Type	Size	Default
compress	Enable/disable data compression.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable compress		
	<i>disable</i>	Disable compress		
eip	End IP.	ipv4-address	Not Specified	0.0.0.0
enforce-ipsec	Enable/disable IPsec enforcement.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable enforce-ipsec		
	<i>disable</i>	Disable enforce-ipsec		

Parameter	Description	Type	Size	Default
hello-interval	L2TP hello message interval in seconds.	integer	Minimum value: 0 Maximum value: 3600	60
lcp-echo-interval	Time in seconds between PPPoE Link Control Protocol (LCP) echo requests.	integer	Minimum value: 0 Maximum value: 32767	5
lcp-max-echo-fails	Maximum number of missed LCP echo messages before disconnect.	integer	Minimum value: 0 Maximum value: 32767	3
sip	Start IP.	ipv4-address	Not Specified	0.0.0.0
status	Enable/disable FortiGate as a L2TP gateway.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
usrgrp	User group.	string	Maximum length: 35	

## config vpn ocvpn

Configure Overlay Controller VPN settings.

```

config vpn ocvpn
    Description: Configure Overlay Controller VPN settings.
    set auto-discovery [enable|disable]
    set auto-discovery-shortcut-mode [independent|dependent]
    set eap [enable|disable]
    set eap-users {string}
    config forticlient-access
        Description: Configure FortiClient settings.
        set status [enable|disable]
        set psksecret {password-3}
        config auth-groups
            Description: FortiClient user authentication groups.
            edit <name>
                set auth-group {string}
                set overlays <overlay-name1>, <overlay-name2>, ...
            next
        end
    end
end

```

```

end
set ip-allocation-block {ipv4-classnet-any}
set multipath [enable|disable]
set nat [enable|disable]
config overlays
    Description: Network overlays to register with Overlay Controller VPN service.
    edit <overlay-name>
        set inter-overlay [allow|deny]
        config subnets
            Description: Internal subnets to register with OCVPN service.
            edit <id>
                set type [subnet|interface]
                set subnet {ipv4-classnet-any}
                set interface {string}
            next
        end
    next
end
set poll-interval {integer}
set role [spoke|primary-hub|...]
set sdwan [enable|disable]
set sdwan-zone {string}
set status [enable|disable]
set wan-interface <name1>, <name2>, ...
end

```

## config vpn ocvpn

Parameter	Description	Type	Size	Default						
auto-discovery	Enable/disable auto-discovery shortcuts.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable ADVPN auto-discovery shortcuts.</td></tr><tr><td><i>disable</i></td><td>Disable ADVPN auto-discovery shortcuts.</td></tr></table>	Option	Description	<i>enable</i>	Enable ADVPN auto-discovery shortcuts.	<i>disable</i>	Disable ADVPN auto-discovery shortcuts.			
	Option	Description								
	<i>enable</i>	Enable ADVPN auto-discovery shortcuts.								
<i>disable</i>	Disable ADVPN auto-discovery shortcuts.									
auto-discovery-shortcut-mode	Control deletion of child short-cut tunnels when the parent tunnel goes down.	option	-	independent						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>independent</i></td><td>Short-cut tunnels remain up if the parent tunnel goes down.</td></tr><tr><td><i>dependent</i></td><td>Short-cut tunnels are brought down if the parent tunnel goes down.</td></tr></table>	Option	Description	<i>independent</i>	Short-cut tunnels remain up if the parent tunnel goes down.	<i>dependent</i>	Short-cut tunnels are brought down if the parent tunnel goes down.			
	Option	Description								
	<i>independent</i>	Short-cut tunnels remain up if the parent tunnel goes down.								
<i>dependent</i>	Short-cut tunnels are brought down if the parent tunnel goes down.									
eap	Enable/disable EAP client authentication.	option	-	disable						

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable EAP client authentication.		
	<i>disable</i>	Disable EAP client authentication.		
eap-users	EAP authentication user group.	string	Maximum length: 35	
ip-allocation-block	Class B subnet reserved for private IP address assignment.	ipv4-classnet-any	Not Specified	10.254.0.0 255.255.0.0
multipath	Enable/disable multipath redundancy.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable multipath redundancy.		
	<i>disable</i>	Disable multipath redundancy.		
nat	Enable/disable NAT support.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable NAT support.		
	<i>disable</i>	Disable NAT support.		
poll-interval	Overlay Controller VPN polling interval.	integer	Minimum value: 30 Maximum value: 120	30
role	Set device role.	option	-	spoke
	<b>Option</b>	<b>Description</b>		
	<i>spoke</i>	Register device as static spoke.		
	<i>primary-hub</i>	Register device as primary hub.		
	<i>secondary-hub</i>	Register device as secondary hub.		
sdwan	Enable/disable adding OCVPN tunnels to SD-WAN.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable adding OCVPN tunnels to SD-WAN.		
	<i>disable</i>	Disable adding OCVPN tunnels to SD-WAN.		

Parameter	Description	Type	Size	Default
sdwan-zone	Set SD-WAN zone.	string	Maximum length: 35	virtual-wan-link
status	Enable/disable Overlay Controller cloud assisted VPN.	option	-	disable
	Option	Description		
	enable	Enable Overlay Controller VPN.		
	disable	Disable Overlay Controller VPN.		
wan-interface <name>	FortiGate WAN interfaces to use with OCVPN. Interface name.	string	Maximum length: 79	

### config forticlient-access

Parameter	Description	Type	Size	Default
status	Enable/disable FortiClient to access OCVPN networks.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable FortiClient access to OCVPN overlays.		
	<i>disable</i>	Disable FortiClient access to OCVPN overlays.		
psksecret	Pre-shared secret for FortiClient PSK authentication (ASCII string or hexadecimal encoded with a leading 0x).	password-3	Not Specified	

### config auth-groups

Parameter	Description	Type	Size	Default
name	Group name.	string	Maximum length: 35	
auth-group	Authentication user group for FortiClient access.	string	Maximum length: 35	
overlays <overlay-name>	OCVPN overlays to allow access to. Overlay name.	string	Maximum length: 79	



## config overlays

Parameter	Description	Type	Size	Default
overlay-name	Overlay name.	string	Maximum length: 63	
inter-overlay	Allow or deny traffic from other overlays.	option	-	deny
	Option	Description		
	allow	Allow traffic from other overlays.		
	deny	Deny traffic from other overlays.		

## config subnets

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
type	Subnet type.	option	-	subnet
	<div><div>Option</div><div>Description</div></div>			
	<div><div>subnet</div><div>Configure participating subnet IP and mask.</div></div>			
	<div><div>interface</div><div>Configure participating LAN interface.</div></div>			
subnet	IPv4 address and subnet mask.	ipv4-classnet-any	Not Specified	0.0.0.0 0.0.0.0
interface	LAN interface.	string	Maximum length: 15	

## config vpn pptp

Configure PPTP.

```
config vpn pptp
  Description: Configure PPTP.
  set eip {ipv4-address}
  set ip-mode [range|usrgrp]
  set local-ip {ipv4-address}
  set sip {ipv4-address}
  set status [enable|disable]
  set usrgrp {string}
end
```

## config vpn pptp

Parameter	Description	Type	Size	Default
eip	End IP.	ipv4-address	Not Specified	0.0.0.0
ip-mode	IP assignment mode for PPTP client.	option	-	range
	<b>Option</b>	<b>Description</b>		
	<i>range</i>	PPTP client IP from manual config (range from sip to eip).		
	<i>usrgrp</i>	PPTP client IP from user-group defined server.		
local-ip	Local IP to be used for peer's remote IP.	ipv4-address	Not Specified	0.0.0.0
sip	Start IP.	ipv4-address	Not Specified	0.0.0.0
status	Enable/disable FortiGate as a PPTP gateway.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
usrgrp	User group.	string	Maximum length: 35	

## config vpn ssl client

Client.

```
config vpn ssl client
  Description: Client.
  edit <name>
    set certificate {string}
    set comment {var-string}
    set distance {integer}
    set interface {string}
    set peer {string}
    set port {integer}
    set priority {integer}
    set psk {password-3}
    set realm {string}
    set server {string}
    set source-ip {string}
    set status [enable|disable]
    set user {string}
  next
end
```

## config vpn ssl client

Parameter	Description	Type	Size	Default
certificate	Certificate to offer to SSL-VPN server if it requests one.	string	Maximum length: 35	
comment	Comment.	var-string	Maximum length: 255	
distance	Distance for routes added by SSL-VPN.	integer	Minimum value: 1 Maximum value: 255	10
interface	SSL interface to send/receive traffic over.	string	Maximum length: 15	
name	SSL-VPN tunnel name.	string	Maximum length: 35	
peer	Authenticate peer's certificate with the peer/peergrp.	string	Maximum length: 35	
port	SSL-VPN server port.	integer	Minimum value: 1 Maximum value: 65535	443
priority	Priority for routes added by SSL-VPN.	integer	Minimum value: 1 Maximum value: 65535	1
psk	Pre-shared secret to authenticate with the server (ASCII string or hexadecimal encoded with a leading 0x).	password-3	Not Specified	
realm	Realm name configured on SSL-VPN server.	string	Maximum length: 35	
server	IPv4, IPv6 or DNS address of the SSL-VPN server.	string	Maximum length: 63	
source-ip	IPv4 or IPv6 address to use as a source for the SSL-VPN connection to the server.	string	Maximum length: 63	
status	Enable/disable this SSL-VPN client configuration.	option	-	enable
		Option	Description	
		<i>enable</i>	Enable the SSL-VPN configuration.	
		<i>disable</i>	Disable the SSL-VPN configuration.	

Parameter	Description	Type	Size	Default
user	Username to offer to the peer to authenticate the client.	string	Maximum length: 35	

## config vpn ssl settings

Configure SSL-VPN.

```
config vpn ssl settings
    Description: Configure SSL-VPN.
    set algorithm [high|medium|...]
    set auth-session-check-source-ip [enable|disable]
    set auth-timeout {integer}
    config authentication-rule
        Description: Authentication rule for SSL-VPN.
        edit <id>
            set source-interface <name1>, <name2>, ...
            set source-address <name1>, <name2>, ...
            set source-address-negate [enable|disable]
            set source-address6 <name1>, <name2>, ...
            set source-address6-negate [enable|disable]
            set users <name1>, <name2>, ...
            set groups <name1>, <name2>, ...
            set portal {string}
            set realm {string}
            set client-cert [enable|disable]
            set user-peer {string}
            set cipher [any|high|...]
            set auth [any|local|...]
        next
    end
    set auto-tunnel-static-route [enable|disable]
    set banned-cipher {option1}, {option2}, ...
    set check-referer [enable|disable]
    set ciphersuite {option1}, {option2}, ...
    set client-sigalgs [no-rsa-pss|all]
    set default-portal {string}
    set deflate-compression-level {integer}
    set deflate-min-data-size {integer}
    set dns-server1 {ipv4-address}
    set dns-server2 {ipv4-address}
    set dns-suffix {var-string}
    set dtls-hello-timeout {integer}
    set dtls-max-proto-ver [dtls1-0|dtls1-2]
    set dtls-min-proto-ver [dtls1-0|dtls1-2]
    set dtls-tunnel [enable|disable]
    set dual-stack-mode [enable|disable]
    set encode-2f-sequence [enable|disable]
    set encrypt-and-store-password [enable|disable]
    set force-two-factor-auth [enable|disable]
    set header-x-forwarded-for [pass|add|...]
    set hsts-include-subdomains [enable|disable]
    set http-compression [enable|disable]
```

```

set http-only-cookie [enable|disable]
set http-request-body-timeout {integer}
set http-request-header-timeout {integer}
set https-redirect [enable|disable]
set idle-timeout {integer}
set ipv6-dns-server1 {ipv6-address}
set ipv6-dns-server2 {ipv6-address}
set ipv6-wins-server1 {ipv6-address}
set ipv6-wins-server2 {ipv6-address}
set login-attempt-limit {integer}
set login-block-time {integer}
set login-timeout {integer}
set port {integer}
set port-precedence [enable|disable]
set reqclientcert [enable|disable]
set saml-redirect-port {integer}
set servercert {string}
set source-address <name1>, <name2>, ...
set source-address-negate [enable|disable]
set source-address6 <name1>, <name2>, ...
set source-address6-negate [enable|disable]
set source-interface <name1>, <name2>, ...
set ssl-client-renegotiation [disable|enable]
set ssl-insert-empty-fragment [enable|disable]
set ssl-max-proto-ver [tls1-0|tls1-1|...]
set ssl-min-proto-ver [tls1-0|tls1-1|...]
set status [enable|disable]
set transform-backward-slashes [enable|disable]
set tunnel-addr-assigned-method [first-available|round-robin]
set tunnel-connect-without-reauth [enable|disable]
set tunnel-ip-pools <name1>, <name2>, ...
set tunnel-ipv6-pools <name1>, <name2>, ...
set tunnel-user-session-timeout {integer}
set unsafe-legacy-renegotiation [enable|disable]
set url-obscuration [enable|disable]
set user-peer {string}
set wins-server1 {ipv4-address}
set wins-server2 {ipv4-address}
set x-content-type-options [enable|disable]

```

end

## config vpn ssl settings

Parameter	Description	Type	Size	Default
algorithm	Force the SSL-VPN security level. High allows only high. Medium allows medium and high. Low allows any.	option	-	high
</				

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>medium</i>	High and medium algorithms.		
	<i>default</i>	default		
	<i>low</i>	All algorithms.		
auth-session-check-source-ip	Enable/disable checking of source IP for authentication session.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable checking of source IP for authentication session.		
	<i>disable</i>	Disable checking of source IP for authentication session.		
auth-timeout	SSL-VPN authentication timeout.	integer	Minimum value: 0 Maximum value: 259200	28800
auto-tunnel-static-route	Enable/disable to auto-create static routes for the SSL-VPN tunnel IP addresses.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
banned-cipher	Select one or more cipher technologies that cannot be used in SSL-VPN negotiations. Only applies to TLS 1.2 and below.	option	-	
	<b>Option</b>	<b>Description</b>		
	<i>RSA</i>	Ban the use of cipher suites using RSA key.		
	<i>DHE</i>	Ban the use of cipher suites using authenticated ephemeral DH key agreement.		
	<i>ECDHE</i>	Ban the use of cipher suites using authenticated ephemeral ECDH key agreement.		
	<i>DSS</i>	Ban the use of cipher suites using DSS authentication.		
	<i>ECDSA</i>	Ban the use of cipher suites using ECDSA authentication.		
	<i>AES</i>	Ban the use of cipher suites using either 128 or 256 bit AES.		
	<i>AESGCM</i>	Ban the use of cipher suites AES in Galois Counter Mode (GCM).		

Parameter	Description	Type	Size	Default																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>CAMELLIA</td><td>Ban the use of cipher suites using either 128 or 256 bit CAMELLIA.</td></tr><tr><td>3DES</td><td>Ban the use of cipher suites using triple DES</td></tr><tr><td>SHA1</td><td>Ban the use of cipher suites using HMAC-SHA1.</td></tr><tr><td>SHA256</td><td>Ban the use of cipher suites using HMAC-SHA256.</td></tr><tr><td>SHA384</td><td>Ban the use of cipher suites using HMAC-SHA384.</td></tr><tr><td>STATIC</td><td>Ban the use of cipher suites using static keys.</td></tr><tr><td>CHACHA20</td><td>Ban the use of cipher suites using ChaCha20.</td></tr><tr><td>ARIA</td><td>Ban the use of cipher suites using ARIA.</td></tr><tr><td>AESCCM</td><td>Ban the use of cipher suites using AESCCM.</td></tr></table>	Option	Description	CAMELLIA	Ban the use of cipher suites using either 128 or 256 bit CAMELLIA.	3DES	Ban the use of cipher suites using triple DES	SHA1	Ban the use of cipher suites using HMAC-SHA1.	SHA256	Ban the use of cipher suites using HMAC-SHA256.	SHA384	Ban the use of cipher suites using HMAC-SHA384.	STATIC	Ban the use of cipher suites using static keys.	CHACHA20	Ban the use of cipher suites using ChaCha20.	ARIA	Ban the use of cipher suites using ARIA.	AESCCM	Ban the use of cipher suites using AESCCM.			
	Option	Description																						
	CAMELLIA	Ban the use of cipher suites using either 128 or 256 bit CAMELLIA.																						
	3DES	Ban the use of cipher suites using triple DES																						
	SHA1	Ban the use of cipher suites using HMAC-SHA1.																						
	SHA256	Ban the use of cipher suites using HMAC-SHA256.																						
	SHA384	Ban the use of cipher suites using HMAC-SHA384.																						
	STATIC	Ban the use of cipher suites using static keys.																						
	CHACHA20	Ban the use of cipher suites using ChaCha20.																						
	ARIA	Ban the use of cipher suites using ARIA.																						
AESCCM	Ban the use of cipher suites using AESCCM.																							
check-referer	Enable/disable verification of referer field in HTTP request header.	option	-	disable																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable verification of referer field in HTTP request header.</td></tr><tr><td>disable</td><td>Disable verification of referer field in HTTP request header.</td></tr></table>	Option	Description	enable	Enable verification of referer field in HTTP request header.	disable	Disable verification of referer field in HTTP request header.																	
	Option	Description																						
	enable	Enable verification of referer field in HTTP request header.																						
disable	Disable verification of referer field in HTTP request header.																							
ciphersuite	Select one or more TLS 1.3 ciphersuites to enable. Does not affect ciphers in TLS 1.2 and below. At least one must be enabled. To disable all, set ssl-max-proto-ver to tls1-2 or below.	option	-	TLS-AES-128-GCM-SHA256 TLS-AES-256-GCM-SHA384 TLS-CHACHA20-POLY1305-SHA256																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>TLS-AES-128-GCM-SHA256</td><td>Enable TLS-AES-128-GCM-SHA256 in TLS 1.3.</td></tr><tr><td>TLS-AES-256-GCM-SHA384</td><td>Enable TLS-AES-256-GCM-SHA384 in TLS 1.3.</td></tr><tr><td>TLS-CHACHA20-POLY1305-SHA256</td><td>Enable TLS-CHACHA20-POLY1305-SHA256 in TLS 1.3.</td></tr></table>	Option	Description	TLS-AES-128-GCM-SHA256	Enable TLS-AES-128-GCM-SHA256 in TLS 1.3.	TLS-AES-256-GCM-SHA384	Enable TLS-AES-256-GCM-SHA384 in TLS 1.3.	TLS-CHACHA20-POLY1305-SHA256	Enable TLS-CHACHA20-POLY1305-SHA256 in TLS 1.3.															
	Option	Description																						
	TLS-AES-128-GCM-SHA256	Enable TLS-AES-128-GCM-SHA256 in TLS 1.3.																						
	TLS-AES-256-GCM-SHA384	Enable TLS-AES-256-GCM-SHA384 in TLS 1.3.																						
TLS-CHACHA20-POLY1305-SHA256	Enable TLS-CHACHA20-POLY1305-SHA256 in TLS 1.3.																							

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>TLS-AES-128-CCM-SHA256</i></td><td>Enable TLS-AES-128-CCM-SHA256 in TLS 1.3.</td></tr><tr><td><i>TLS-AES-128-CCM-8-SHA256</i></td><td>Enable TLS-AES-128-CCM-8-SHA256 in TLS 1.3.</td></tr></table>	Option	Description	<i>TLS-AES-128-CCM-SHA256</i>	Enable TLS-AES-128-CCM-SHA256 in TLS 1.3.	<i>TLS-AES-128-CCM-8-SHA256</i>	Enable TLS-AES-128-CCM-8-SHA256 in TLS 1.3.			
	Option	Description								
	<i>TLS-AES-128-CCM-SHA256</i>	Enable TLS-AES-128-CCM-SHA256 in TLS 1.3.								
<i>TLS-AES-128-CCM-8-SHA256</i>	Enable TLS-AES-128-CCM-8-SHA256 in TLS 1.3.									
client-sigalgs	Set signature algorithms related to client authentication. Affects TLS version <= 1.2 only.	option	-	all						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>no-rsa-pss</i></td><td>Disable RSA-PSS signature algorithms for client authentication.</td></tr><tr><td><i>all</i></td><td>Enable all supported signature algorithms for client authentication.</td></tr></table>	Option	Description	<i>no-rsa-pss</i>	Disable RSA-PSS signature algorithms for client authentication.	<i>all</i>	Enable all supported signature algorithms for client authentication.			
	Option	Description								
	<i>no-rsa-pss</i>	Disable RSA-PSS signature algorithms for client authentication.								
<i>all</i>	Enable all supported signature algorithms for client authentication.									
default-portal	Default SSL-VPN portal.	string	Maximum length: 35							
deflate-compression-level	Compression level (0~9).	integer	Minimum value: 0 Maximum value: 9	6						
deflate-min-data-size	Minimum amount of data that triggers compression.	integer	Minimum value: 200 Maximum value: 65535	300						
dns-server1	DNS server 1.	ipv4-address	Not Specified	0.0.0.0						
dns-server2	DNS server 2.	ipv4-address	Not Specified	0.0.0.0						
dns-suffix	DNS suffix used for SSL-VPN clients.	var-string	Maximum length: 253							
dtls-hello-timeout	SSLVPN maximum DTLS hello timeout.	integer	Minimum value: 10 Maximum value: 60	10						
dtls-max-protocol-ver	DTLS maximum protocol version.	option	-	dtls1-2						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>dtls1-0</i></td><td>DTLS version 1.0.</td></tr><tr><td><i>dtls1-2</i></td><td>DTLS version 1.2.</td></tr></table>	Option	Description	<i>dtls1-0</i>	DTLS version 1.0.	<i>dtls1-2</i>	DTLS version 1.2.			
	Option	Description								
	<i>dtls1-0</i>	DTLS version 1.0.								
<i>dtls1-2</i>	DTLS version 1.2.									



Parameter	Description	Type	Size	Default						
dtls-min-protocol-ver	DTLS minimum protocol version.	option	-	dtls1-0						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>dtls1-0</td><td>DTLS version 1.0.</td></tr><tr><td>dtls1-2</td><td>DTLS version 1.2.</td></tr></table>	Option	Description	dtls1-0	DTLS version 1.0.	dtls1-2	DTLS version 1.2.			
Option	Description									
dtls1-0	DTLS version 1.0.									
dtls1-2	DTLS version 1.2.									
dtls-tunnel	Enable/disable DTLS to prevent eavesdropping, tampering, or message forgery.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>	Option	Description	enable	Enable setting.	disable	Disable setting.			
Option	Description									
enable	Enable setting.									
disable	Disable setting.									
dual-stack-mode	Tunnel mode: enable parallel IPv4 and IPv6 tunnel. Web mode: support IPv4 and IPv6 bookmarks in the portal.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>	Option	Description	enable	Enable setting.	disable	Disable setting.			
Option	Description									
enable	Enable setting.									
disable	Disable setting.									
encode-2f-sequence	Encode \2F sequence to forward slash in URLs.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>	Option	Description	enable	Enable setting.	disable	Disable setting.			
Option	Description									
enable	Enable setting.									
disable	Disable setting.									
encrypt-and-store-password	Encrypt and store user passwords for SSL-VPN web sessions.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>	Option	Description	enable	Enable setting.	disable	Disable setting.			
Option	Description									
enable	Enable setting.									
disable	Disable setting.									
force-two-factor-auth	Enable/disable only PKI users with two-factor authentication for SSL-VPNs.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr></table>	Option	Description	enable	Enable setting.					
Option	Description									
enable	Enable setting.									

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>disable</i>	Disable setting.							
	Option	Description										
<i>disable</i>	Disable setting.											
header-x-forwarded-for	Forward the same, add, or remove HTTP header.	option	-	add								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>pass</i></td><td>Forward the same HTTP header.</td></tr><tr><td><i>add</i></td><td>Add the HTTP header.</td></tr><tr><td><i>remove</i></td><td>Remove the HTTP header.</td></tr></table>	Option	Description	<i>pass</i>	Forward the same HTTP header.	<i>add</i>	Add the HTTP header.	<i>remove</i>	Remove the HTTP header.			
	Option	Description										
	<i>pass</i>	Forward the same HTTP header.										
	<i>add</i>	Add the HTTP header.										
<i>remove</i>	Remove the HTTP header.											
hsts-include-subdomains	Add HSTS includeSubDomains response header.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
	Option	Description										
	<i>enable</i>	Enable setting.										
<i>disable</i>	Disable setting.											
http-compression	Enable/disable to allow HTTP compression over SSL-VPN tunnels.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
	Option	Description										
	<i>enable</i>	Enable setting.										
<i>disable</i>	Disable setting.											
http-only-cookie	Enable/disable SSL-VPN support for HttpOnly cookies.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.					
	Option	Description										
	<i>enable</i>	Enable setting.										
<i>disable</i>	Disable setting.											
http-request-body-timeout	SSL-VPN session is disconnected if an HTTP request body is not received within this time.	integer	Minimum value: 0 Maximum value: 4294967295	30								

Parameter	Description	Type	Size	Default
http-request-header-timeout	SSL-VPN session is disconnected if an HTTP request header is not received within this time.	integer	Minimum value: 0 Maximum value: 4294967295	20
https-redirect	Enable/disable redirect of port 80 to SSL-VPN port.	option	-	disable
	Option	Description		
	enable	Enable setting.		
	disable	Disable setting.		
idle-timeout	SSL-VPN disconnects if idle for specified time in seconds.	integer	Minimum value: 0 Maximum value: 259200	300
ipv6-dns-server1	IPv6 DNS server 1.	ipv6-address	Not Specified	::
ipv6-dns-server2	IPv6 DNS server 2.	ipv6-address	Not Specified	::
ipv6-wins-server1	IPv6 WINS server 1.	ipv6-address	Not Specified	::
ipv6-wins-server2	IPv6 WINS server 2.	ipv6-address	Not Specified	::
login-attempt-limit	SSL-VPN maximum login attempt times before block.	integer	Minimum value: 0 Maximum value: 4294967295	2
login-block-time	Time for which a user is blocked from logging in after too many failed login attempts.	integer	Minimum value: 0 Maximum value: 4294967295	60
login-timeout	SSLVPN maximum login timeout.	integer	Minimum value: 10 Maximum value: 180	30

Parameter	Description	Type	Size	Default						
port	SSL-VPN access port.	integer	Minimum value: 1 Maximum value: 65535	10443						
port-precedence	Enable/disable, Enable means that if SSL-VPN connections are allowed on an interface admin GUI connections are blocked on that interface.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>	Option	Description	enable	Enable setting.	disable	Disable setting.			
Option	Description									
enable	Enable setting.									
disable	Disable setting.									
reqclientcert	Enable/disable to require client certificates for all SSL-VPN users.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>	Option	Description	enable	Enable setting.	disable	Disable setting.			
Option	Description									
enable	Enable setting.									
disable	Disable setting.									
saml-redirect-port	SAML local redirect port in the machine running FortiClient. 0 is to disable redirection on FGT side.	integer	Minimum value: 0 Maximum value: 65535	8020						
servercert	Name of the server certificate to be used for SSL-VPNs.	string	Maximum length: 35							
source-address <name>	Source address of incoming traffic. Address name.	string	Maximum length: 79							
source-address-negate	Enable/disable negated source address match.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>	Option	Description	enable	Enable setting.	disable	Disable setting.			
Option	Description									
enable	Enable setting.									
disable	Disable setting.									
source-address6 <name>	IPv6 source address of incoming traffic. IPv6 address name.	string	Maximum length: 79							
source-address6-negate	Enable/disable negated source IPv6 address match.	option	-	disable						

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
source-interface <name>	SSL-VPN source interface of incoming traffic. Interface name.	string	Maximum length: 35	
ssl-client-renegotiation	Enable/disable to allow client renegotiation by the server if the tunnel goes down.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Abort any SSL connection that attempts to renegotiate.		
	<i>enable</i>	Allow a SSL client to renegotiate.		
ssl-insert-empty-fragment	Enable/disable insertion of empty fragment.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
ssl-max-protocol-ver	SSL maximum protocol version.	option	-	tls1-3
	<b>Option</b>	<b>Description</b>		
	<i>tls1-0</i>	TLS version 1.0.		
	<i>tls1-1</i>	TLS version 1.1.		
	<i>tls1-2</i>	TLS version 1.2.		
	<i>tls1-3</i>	TLS version 1.3.		
ssl-min-protocol-ver	SSL minimum protocol version.	option	-	tls1-2
	<b>Option</b>	<b>Description</b>		
	<i>tls1-0</i>	TLS version 1.0.		
	<i>tls1-1</i>	TLS version 1.1.		
	<i>tls1-2</i>	TLS version 1.2.		
	<i>tls1-3</i>	TLS version 1.3.		
status	Enable/disable SSL-VPN.	option	-	enable

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable SSL-VPN.</td></tr><tr><td><i>disable</i></td><td>Disable SSL-VPN.</td></tr></table>	Option	Description	<i>enable</i>	Enable SSL-VPN.	<i>disable</i>	Disable SSL-VPN.			
	Option	Description								
	<i>enable</i>	Enable SSL-VPN.								
<i>disable</i>	Disable SSL-VPN.									
transform-backward-slashes	Transform backward slashes to forward slashes in URLs.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
	Option	Description								
	<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.									
tunnel-addr-assigned-method	Method used for assigning address for tunnel.	option	-	first-available						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>first-available</i></td><td>Assign the first available address from the pools.</td></tr><tr><td><i>round-robin</i></td><td>Assign the available address from the pool with a round robin fashion.</td></tr></table>	Option	Description	<i>first-available</i>	Assign the first available address from the pools.	<i>round-robin</i>	Assign the available address from the pool with a round robin fashion.			
	Option	Description								
	<i>first-available</i>	Assign the first available address from the pools.								
<i>round-robin</i>	Assign the available address from the pool with a round robin fashion.									
tunnel-connect-without-reauth	Enable/disable tunnel connection without re-authorization if previous connection dropped.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable tunnel connection without re-authorization.</td></tr><tr><td><i>disable</i></td><td>Disable tunnel connection without re-authorization.</td></tr></table>	Option	Description	<i>enable</i>	Enable tunnel connection without re-authorization.	<i>disable</i>	Disable tunnel connection without re-authorization.			
	Option	Description								
	<i>enable</i>	Enable tunnel connection without re-authorization.								
<i>disable</i>	Disable tunnel connection without re-authorization.									
tunnel-ip-pools <name>	Names of the IPv4 IP Pool firewall objects that define the IP addresses reserved for remote clients. Address name.	string	Maximum length: 79							
tunnel-ipv6-pools <name>	Names of the IPv6 IP Pool firewall objects that define the IP addresses reserved for remote clients. Address name.	string	Maximum length: 79							
tunnel-user-session-timeout	Time out value to clean up user session after tunnel connection is dropped.	integer	Minimum value: 1 Maximum value: 255	30						

Parameter	Description	Type	Size	Default
unsafe-legacy-renegotiation	Enable/disable unsafe legacy re-negotiation.	option	-	disable
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
url-obscuration	Enable/disable to obscure the host name of the URL of the web browser display.	option	-	disable
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
user-peer	Name of user peer.	string	Maximum length: 35	
wins-server1	WINS server 1.	ipv4-address	Not Specified	0.0.0.0
wins-server2	WINS server 2.	ipv4-address	Not Specified	0.0.0.0
x-content-type-options	Add HTTP X-Content-Type-Options header.	option	-	enable
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

### config authentication-rule

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
source-interface <name>	SSL-VPN source interface of incoming traffic. Interface name.	string	Maximum length: 35	
source-address <name>	Source address of incoming traffic. Address name.	string	Maximum length: 79	

Parameter	Description	Type	Size	Default						
source-address-negate	Enable/disable negated source address match.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
source-address6 <name>	IPv6 source address of incoming traffic. IPv6 address name.	string	Maximum length: 79							
source-address6-negate	Enable/disable negated source IPv6 address match.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
users <name>	User name. User name.	string	Maximum length: 79							
groups <name>	User groups. Group name.	string	Maximum length: 79							
portal	SSL-VPN portal.	string	Maximum length: 35							
realm	SSL-VPN realm.	string	Maximum length: 35							
client-cert	Enable/disable SSL-VPN client certificate restrictive.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
user-peer	Name of user peer.	string	Maximum length: 35							
cipher	SSL-VPN cipher strength.	option	-	high						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>any</i></td><td>Any cipher strength.</td></tr></table>	Option	Description	<i>any</i>	Any cipher strength.					
Option	Description									
<i>any</i>	Any cipher strength.									



Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>high</i>	High cipher strength (>= 168 bits).		
	<i>medium</i>	Medium cipher strength (>= 128 bits).		
auth	SSL-VPN authentication method restriction.	option	-	any
	<b>Option</b>	<b>Description</b>		
	<i>any</i>	Any		
	<i>local</i>	Local		
	<i>radius</i>	RADIUS		
	<i>tacacs+</i>	TACACS+		
	<i>ldap</i>	LDAP		
	<i>peer</i>	PEER		

## config vpn ssl web host-check-software

SSL-VPN host check software.

```

config vpn ssl web host-check-software
    Description: SSL-VPN host check software.
    edit <name>
        config check-item-list
            Description: Check item list.
            edit <id>
                set action [require|deny]
                set type [file|registry|...]
                set target {string}
                set version {string}
                set md5s <id1>, <id2>, ...
            next
        end
        set guid {user}
        set os-type [windows|macos]
        set type [av|fw]
        set version {string}
    next
end

```

## config vpn ssl web host-check-software

Parameter	Description	Type	Size	Default						
guid	Globally unique ID.	user	Not Specified							
name	Name.	string	Maximum length: 63							
os-type	OS type.	option	-	windows						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>windows</td><td>Microsoft Windows operating system.</td></tr><tr><td>macos</td><td>Apple MacOS operating system.</td></tr></table>				Option	Description	windows	Microsoft Windows operating system.	macos	Apple MacOS operating system.
	Option	Description								
	windows	Microsoft Windows operating system.								
macos	Apple MacOS operating system.									
type	Type.	option	-	av						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>av</td><td>AntiVirus.</td></tr><tr><td>fw</td><td>Firewall.</td></tr></table>				Option	Description	av	AntiVirus.	fw	Firewall.
	Option	Description								
	av	AntiVirus.								
fw	Firewall.									
version	Version.	string	Maximum length: 35							

## config check-item-list

Parameter	Description	Type	Size	Default						
id	ID.	integer	Minimum value: 0 Maximum value: 65535	0						
action	Action.	option	-	require						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>require</i></td><td>Require.</td></tr><tr><td><i>deny</i></td><td>Deny.</td></tr></table>				Option	Description	<i>require</i>	Require.	<i>deny</i>	Deny.
	Option	Description								
	<i>require</i>	Require.								
<i>deny</i>	Deny.									
type	Type.	option	-	file						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>file</i></td><td>File.</td></tr></table>				Option	Description	<i>file</i>	File.		
	Option	Description								
<i>file</i>	File.									

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>registry</i>	Registry.		
	<i>process</i>	Process.		
target	Target.	string	Maximum length: 255	
version	Version.	string	Maximum length: 35	
md5s <id>	MD5 checksum. Hex string of MD5 checksum.	string	Maximum length: 32	

## config vpn ssl web portal

Portal.

```

config vpn ssl web portal
  Description: Portal.
  edit <name>
    set allow-user-access {option1}, {option2}, ...
    set auto-connect [enable|disable]
    config bookmark-group
      Description: Portal bookmark group.
      edit <name>
        config bookmarks
          Description: Bookmark table.
          edit <name>
            set apptype [ftp|rdp|...]
            set url {var-string}
            set host {var-string}
            set folder {var-string}
            set domain {var-string}
            set additional-params {var-string}
            set description {var-string}
            set keyboard-layout [ar-101|ar-102|...]
            set security [any|rdp|...]
            set send-preconnection-id [enable|disable]
            set preconnection-id {integer}
            set preconnection-blob {var-string}
            set load-balancing-info {var-string}
            set restricted-admin [enable|disable]
            set port {integer}
            set logon-user {var-string}
            set logon-password {password}
            set color-depth [32|16|...]
            set sso [disable|static|...]
          config form-data
            Description: Form data.
            edit <name>

```

```

        set value {var-string}
    next
end
set sso-credential [sslvpn-login|alternative]
set sso-username {var-string}
set sso-password {password}
set sso-credential-sent-once [enable|disable]
set width {integer}
set height {integer}
next
end
next
end
set clipboard [enable|disable]
set custom-lang {string}
set customize-forticlient-download-url [enable|disable]
set default-window-height {integer}
set default-window-width {integer}
set dhcp-ip-overlap [use-new|use-old]
set display-bookmark [enable|disable]
set display-connection-tools [enable|disable]
set display-history [enable|disable]
set display-status [enable|disable]
set dns-server1 {ipv4-address}
set dns-server2 {ipv4-address}
set dns-suffix {var-string}
set exclusive-routing [enable|disable]
set forticlient-download [enable|disable]
set forticlient-download-method [direct|ssl-vpn]
set heading {string}
set hide-sso-credential [enable|disable]
set host-check [none|av|...]
set host-check-interval {integer}
set host-check-policy <name1>, <name2>, ...
set ip-mode [range|user-group|...]
set ip-pools <name1>, <name2>, ...
set ipv6-dns-server1 {ipv6-address}
set ipv6-dns-server2 {ipv6-address}
set ipv6-exclusive-routing [enable|disable]
set ipv6-pools <name1>, <name2>, ...
set ipv6-service-restriction [enable|disable]
set ipv6-split-tunneling [enable|disable]
set ipv6-split-tunneling-routing-address <name1>, <name2>, ...
set ipv6-split-tunneling-routing-negate [enable|disable]
set ipv6-tunnel-mode [enable|disable]
set ipv6-wins-server1 {ipv6-address}
set ipv6-wins-server2 {ipv6-address}
set keep-alive [enable|disable]
set limit-user-logins [enable|disable]
set mac-addr-action [allow|deny]
set mac-addr-check [enable|disable]
config mac-addr-check-rule
    Description: Client MAC address check rule.
    edit <name>
        set mac-addr-mask {integer}
        set mac-addr-list <addr1>, <addr2>, ...

```

```

        next
    end
    set macos-forticlient-download-url {var-string}
    set os-check [enable|disable]
    config os-check-list
        Description: SSL-VPN OS checks.
        edit <name>
            set action [deny|allow|...]
            set tolerance {integer}
            set latest-patch-level {user}
        next
    end
    set prefer-ipv6-dns [enable|disable]
    set redirect-url {var-string}
    set rewrite-ip-uri-ui [enable|disable]
    set save-password [enable|disable]
    set service-restriction [enable|disable]
    set skip-check-for-browser [enable|disable]
    set skip-check-for-unsupported-os [enable|disable]
    set smb-max-version [smbv1|smbv2|...]
    set smb-min-version [smbv1|smbv2|...]
    set smb-ntlmv1-auth [enable|disable]
    set smbv1 [enable|disable]
    config split-dns
        Description: Split DNS for SSL-VPN.
        edit <id>
            set domains {var-string}
            set dns-server1 {ipv4-address}
            set dns-server2 {ipv4-address}
            set ipv6-dns-server1 {ipv6-address}
            set ipv6-dns-server2 {ipv6-address}
        next
    end
    set split-tunneling [enable|disable]
    set split-tunneling-routing-address <name1>, <name2>, ...
    set split-tunneling-routing-negate [enable|disable]
    set theme [jade|neutrino|...]
    set tunnel-mode [enable|disable]
    set use-sdwan [enable|disable]
    set user-bookmark [enable|disable]
    set user-group-bookmark [enable|disable]
    set web-mode [enable|disable]
    set windows-forticlient-download-url {var-string}
    set wins-server1 {ipv4-address}
    set wins-server2 {ipv4-address}
next
end

```

## config vpn ssl web portal

Parameter	Description	Type	Size	Default
allow-user-access	Allow user access to SSL-VPN applications.	option	-	web ftp smb sftp telnet ssh vnc rdp ping
	<b>Option</b>	<b>Description</b>		
	<i>web</i>	HTTP/HTTPS access.		
	<i>ftp</i>	FTP access.		
	<i>smb</i>	SMB/CIFS access.		
	<i>sftp</i>	SFTP access.		
	<i>telnet</i>	TELNET access.		
	<i>ssh</i>	SSH access.		
	<i>vnc</i>	VNC access.		
	<i>rdp</i>	RDP access.		
	<i>ping</i>	PING access.		
auto-connect	Enable/disable automatic connect by client when system is up.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
clipboard	Enable to support RDP/VPC clipboard functionality.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable support of RDP/VNC clipboard.		
	<i>disable</i>	Disable support of RDP/VNC clipboard.		
custom-lang	Change the web portal display language. Overrides config system global set language. You can use config system custom-language and execute system custom-language to add custom language files.	string	Maximum length: 35	
customize-forticlient-download-url	Enable support of customized download URL for FortiClient.	option	-	disable

Parameter	Description	Type	Size	Default
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
default-window-height	Screen height.	integer	Minimum value: 0 Maximum value: 65535	768
default-window-width	Screen width.	integer	Minimum value: 0 Maximum value: 65535	1024
dhcp-ip-overlap	Configure overlapping DHCP IP allocation assignment.	option	-	use-new
	<b>Option</b> <b>Description</b>			
	<i>use-new</i>	Assign DHCP lease to new client and remove old client lease.		
	<i>use-old</i>	Preserve previous client IP allocation and disconnect new client.		
display-bookmark	Enable to display the web portal bookmark widget.	option	-	enable
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
display-connection-tools	Enable to display the web portal connection tools widget.	option	-	enable
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
display-history	Enable to display the web portal user login history widget.	option	-	enable

Parameter	Description	Type	Size	Default
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
display-status	Enable to display the web portal status widget.	option	-	enable
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
dns-server1	IPv4 DNS server 1.	ipv4-address	Not Specified	0.0.0.0
dns-server2	IPv4 DNS server 2.	ipv4-address	Not Specified	0.0.0.0
dns-suffix	DNS suffix.	var-string	Maximum length: 253	
exclusive-routing	Enable/disable all traffic go through tunnel only.	option	-	disable
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
forticlient-download	Enable/disable download option for FortiClient.	option	-	enable
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
forticlient-download-method	FortiClient download method.	option	-	direct
	<b>Option</b> <b>Description</b>			
	<i>direct</i>	Download via direct link.		
	<i>ssl-vpn</i>	Download via SSL-VPN.		
heading	Web portal heading message.	string	Maximum length: 31	SSL-VPN Portal



Parameter	Description	Type	Size	Default												
hide-ssocredential	Enable to prevent SSO credential being sent to client.	option	-	enable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>	Option	Description	enable	Enable setting.	disable	Disable setting.									
Option	Description															
enable	Enable setting.															
disable	Disable setting.															
host-check	Type of host checking performed on endpoints.	option	-	none												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>none</td><td>No host checking.</td></tr><tr><td>av</td><td>AntiVirus software recognized by the Windows Security Center.</td></tr><tr><td>fw</td><td>Firewall software recognized by the Windows Security Center.</td></tr><tr><td>av-fw</td><td>AntiVirus and firewall software recognized by the Windows Security Center.</td></tr><tr><td>custom</td><td>Custom.</td></tr></table>	Option	Description	none	No host checking.	av	AntiVirus software recognized by the Windows Security Center.	fw	Firewall software recognized by the Windows Security Center.	av-fw	AntiVirus and firewall software recognized by the Windows Security Center.	custom	Custom.			
Option	Description															
none	No host checking.															
av	AntiVirus software recognized by the Windows Security Center.															
fw	Firewall software recognized by the Windows Security Center.															
av-fw	AntiVirus and firewall software recognized by the Windows Security Center.															
custom	Custom.															
host-check-interval	Periodic host check interval. Value of 0 means disabled and host checking only happens when the endpoint connects.	integer	Minimum value: 120 Maximum value: 259200	0												
host-check-policy <name>	One or more policies to require the endpoint to have specific security software. Host check software list name.	string	Maximum length: 79													
ip-mode	Method by which users of this SSL-VPN tunnel obtain IP addresses.	option	-	range												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>range</td><td>Use the IP addresses available for all SSL-VPN users as defined by the SSL settings command.</td></tr><tr><td>user-group</td><td>Use the IP addresses associated with individual users or user groups (usually from external auth servers).</td></tr><tr><td>dhcp</td><td>Use IP addresses obtained from external DHCP server.</td></tr></table>	Option	Description	range	Use the IP addresses available for all SSL-VPN users as defined by the SSL settings command.	user-group	Use the IP addresses associated with individual users or user groups (usually from external auth servers).	dhcp	Use IP addresses obtained from external DHCP server.							
Option	Description															
range	Use the IP addresses available for all SSL-VPN users as defined by the SSL settings command.															
user-group	Use the IP addresses associated with individual users or user groups (usually from external auth servers).															
dhcp	Use IP addresses obtained from external DHCP server.															
ip-pools <name>	IPv4 firewall source address objects reserved for SSL-VPN tunnel mode clients. Address name.	string	Maximum length: 79													
ipv6-dns-server1	IPv6 DNS server 1.	ipv6-address	Not Specified	::												

Parameter	Description	Type	Size	Default
ipv6-dns-server2	IPv6 DNS server 2.	ipv6-address	Not Specified	::
ipv6-exclusive-routing	Enable/disable all IPv6 traffic go through tunnel only.	option	-	disable
	Option	Description		
	enable	Enable setting.		
	disable	Disable setting.		
ipv6-pools <name>	IPv6 firewall source address objects reserved for SSL-VPN tunnel mode clients. Address name.	string	Maximum length: 79	
ipv6-service-restriction	Enable/disable IPv6 tunnel service restriction.	option	-	disable
	Option	Description		
	enable	Enable setting.		
	disable	Disable setting.		
ipv6-split-tunneling	Enable/disable IPv6 split tunneling.	option	-	enable
	Option	Description		
	enable	Enable setting.		
	disable	Disable setting.		
ipv6-split-tunneling-routing-address <name>	IPv6 SSL-VPN tunnel mode firewall address objects that override firewall policy destination addresses to control split-tunneling access. Address name.	string	Maximum length: 79	
ipv6-split-tunneling-routing-negate	Enable to negate IPv6 split tunneling routing address.	option	-	disable
	Option	Description		
	enable	Enable setting.		
	disable	Disable setting.		
ipv6-tunnel-mode	Enable/disable IPv6 SSL-VPN tunnel mode.	option	-	disable

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
ipv6-wins-server1	IPv6 WINS server 1.	ipv6-address	Not Specified	::
ipv6-wins-server2	IPv6 WINS server 2.	ipv6-address	Not Specified	::
keep-alive	Enable/disable automatic reconnect for FortiClient connections.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
limit-user-logins	Enable to limit each user to one SSL-VPN session at a time.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
mac-addr-action	Client MAC address action.	option	-	allow
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow connection when client MAC address is matched.		
	<i>deny</i>	Deny connection when client MAC address is matched.		
mac-addr-check	Enable/disable MAC address host checking.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
macos-forticlient-download-url	Download URL for Mac FortiClient.	var-string	Maximum length: 1023	

Parameter	Description	Type	Size	Default						
name	Portal name.	string	Maximum length: 35							
os-check	Enable to let the FortiGate decide action based on client OS.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>	Option	Description	enable	Enable setting.	disable	Disable setting.			
Option	Description									
enable	Enable setting.									
disable	Disable setting.									
prefer-ipv6-dns	Prefer to query IPv6 DNS server first if enabled.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>	Option	Description	enable	Enable setting.	disable	Disable setting.			
Option	Description									
enable	Enable setting.									
disable	Disable setting.									
redir-url	Client login redirect URL.	var-string	Maximum length: 255							
rewrite-ip-uri-ui	Rewrite contents for URI contains IP and /ui/.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable contents rewrite for URI contains "IP-address/ui".</td></tr><tr><td>disable</td><td>Disable contents rewrite for URI contains "IP-address/ui".</td></tr></table>	Option	Description	enable	Enable contents rewrite for URI contains "IP-address/ui".	disable	Disable contents rewrite for URI contains "IP-address/ui".			
Option	Description									
enable	Enable contents rewrite for URI contains "IP-address/ui".									
disable	Disable contents rewrite for URI contains "IP-address/ui".									
save-password	Enable/disable FortiClient saving the user's password.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>	Option	Description	enable	Enable setting.	disable	Disable setting.			
Option	Description									
enable	Enable setting.									
disable	Disable setting.									
service-restriction	Enable/disable tunnel service restriction.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>	Option	Description	enable	Enable setting.	disable	Disable setting.			
Option	Description									
enable	Enable setting.									
disable	Disable setting.									
skip-check-for-browser	Enable to skip host check for browser support.	option	-	enable						

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
skip-check-for-unsupported-os	Enable to skip host check if client OS does not support it.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
smb-max-version	SMB maximum client protocol version.	option	-	smbv3
	<b>Option</b>	<b>Description</b>		
	<i>smbv1</i>	SMB version 1.		
	<i>smbv2</i>	SMB version 2.		
	<i>smbv3</i>	SMB version 3.		
smb-min-version	SMB minimum client protocol version.	option	-	smbv2
	<b>Option</b>	<b>Description</b>		
	<i>smbv1</i>	SMB version 1.		
	<i>smbv2</i>	SMB version 2.		
	<i>smbv3</i>	SMB version 3.		
smb-ntlmv1-auth	Enable support of NTLMv1 for Samba authentication.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
smbv1	SMB version 1.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	enable		
	<i>disable</i>	disable		

Parameter	Description	Type	Size	Default																		
split-tunneling	Enable/disable IPv4 split tunneling.	option	-	enable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.															
	Option	Description																				
	<i>enable</i>	Enable setting.																				
<i>disable</i>	Disable setting.																					
split-tunneling-routing-address <name>	IPv4 SSL-VPN tunnel mode firewall address objects that override firewall policy destination addresses to control split-tunneling access. Address name.	string	Maximum length: 79																			
split-tunneling-routing-negate	Enable to negate split tunneling routing address.	option	-	disable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.															
	Option	Description																				
	<i>enable</i>	Enable setting.																				
<i>disable</i>	Disable setting.																					
theme	Web portal color scheme.	option	-	neutrino																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>jade</i></td><td>Jade theme.</td></tr><tr><td><i>neutrino</i></td><td>Neutrino theme.</td></tr><tr><td><i>mariner</i></td><td>Mariner theme.</td></tr><tr><td><i>graphite</i></td><td>Graphite theme.</td></tr><tr><td><i>melongene</i></td><td>Melongene theme.</td></tr><tr><td><i>dark-matter</i></td><td>Dark Matter theme.</td></tr><tr><td><i>onyx</i></td><td>Onyx theme.</td></tr><tr><td><i>eclipse</i></td><td>Eclipse theme.</td></tr></table>	Option	Description	<i>jade</i>	Jade theme.	<i>neutrino</i>	Neutrino theme.	<i>mariner</i>	Mariner theme.	<i>graphite</i>	Graphite theme.	<i>melongene</i>	Melongene theme.	<i>dark-matter</i>	Dark Matter theme.	<i>onyx</i>	Onyx theme.	<i>eclipse</i>	Eclipse theme.			
	Option	Description																				
	<i>jade</i>	Jade theme.																				
	<i>neutrino</i>	Neutrino theme.																				
	<i>mariner</i>	Mariner theme.																				
	<i>graphite</i>	Graphite theme.																				
	<i>melongene</i>	Melongene theme.																				
	<i>dark-matter</i>	Dark Matter theme.																				
<i>onyx</i>	Onyx theme.																					
<i>eclipse</i>	Eclipse theme.																					
tunnel-mode	Enable/disable IPv4 SSL-VPN tunnel mode.	option	-	disable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.															
	Option	Description																				
	<i>enable</i>	Enable setting.																				
<i>disable</i>	Disable setting.																					
use-sdwan	Use SD-WAN rules to get output interface.	option	-	disable																		

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
user-bookmark	Enable to allow web portal users to create their own bookmarks.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
user-group-bookmark	Enable to allow web portal users to create bookmarks for all users in the same user group.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
web-mode	Enable/disable SSL-VPN web mode.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
windows-forticlient-download-url	Download URL for Windows FortiClient.	var-string	Maximum length: 1023	
wins-server1	IPv4 WINS server 1.	ipv4-address	Not Specified	0.0.0.0
wins-server2	IPv4 WINS server 1.	ipv4-address	Not Specified	0.0.0.0

### config bookmark-group

Parameter	Description	Type	Size	Default
name	Bookmark group name.	string	Maximum length: 35	

## config bookmarks

Parameter	Description	Type	Size	Default
name	Bookmark name.	string	Maximum length: 35	
apptype	Application type.	option	-	web
	OptionDescription			
	ftp	FTP.		
	rdp	RDP.		
	sftp	SFTP.		
	smb	SMB/CIFS.		
	ssh	SSH.		
	telnet	Telnet.		
	vnc	VNC.		
	web	HTTP/HTTPS.		
url	URL parameter.	var-string	Maximum length: 128	
host	Host name/IP parameter.	var-string	Maximum length: 128	
folder	Network shared file folder parameter.	var-string	Maximum length: 128	
domain	Login domain.	var-string	Maximum length: 128	
additional-params	Additional parameters.	var-string	Maximum length: 128	
description	Description.	var-string	Maximum length: 128	
keyboard-layout	Keyboard layout.	option	-	en-us
	OptionDescription			
	ar-101	Arabic (101).		
	ar-102	Arabic (102).		
	ar-102-azerty	Arabic (102) AZERTY.		
	can-mul	Canadian Multilingual Standard.		
	cz	Czech.		



Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>cz-qwerty</i>	Czech (QWERTY).		
	<i>cz-pr</i>	Czech Programmers.		
	<i>da</i>	Danish.		
	<i>nl</i>	Dutch.		
	<i>de</i>	German.		
	<i>de-ch</i>	German, Switzerland.		
	<i>de-ibm</i>	German (IBM).		
	<i>en-uk</i>	English, United Kingdom.		
	<i>en-uk-ext</i>	English, United Kingdom Extended.		
	<i>en-us</i>	English, United States.		
	<i>en-us-dvorak</i>	English, United States-Dvorak.		
	<i>es</i>	Spanish.		
	<i>es-var</i>	Spanish Variation.		
	<i>fi</i>	Finnish.		
	<i>fi-sami</i>	Finnish with Sami.		
	<i>fr</i>	French.		
	<i>fr-apple</i>	French, Apple.		
	<i>fr-ca</i>	French, Canada.		
	<i>fr-ch</i>	French, Switzerland.		
	<i>fr-be</i>	French, Belgium.		
	<i>hr</i>	Croatian.		
	<i>hu</i>	Hungarian.		
	<i>hu-101</i>	Hungarian 101-Key.		
	<i>it</i>	Italian.		
	<i>it-142</i>	Italian (142).		
	<i>ja</i>	Japanese.		
	<i>ko</i>	Korean.		
	<i>lt</i>	Lithuanian.		
	<i>lt-ibm</i>	Lithuanian IBM.		

Parameter	Description	Type	Size	Default																																																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>lt-std</i></td><td>Lithuanian Standard.</td></tr><tr><td><i>lav-std</i></td><td>Latvian (Standard).</td></tr><tr><td><i>lav-leg</i></td><td>Latvian (Legacy).</td></tr><tr><td><i>mk</i></td><td>Macedonian (FYROM).</td></tr><tr><td><i>mk-std</i></td><td>Macedonia (FYROM) - Standard.</td></tr><tr><td><i>no</i></td><td>Norwegian.</td></tr><tr><td><i>no-sami</i></td><td>Norwegian with Sami.</td></tr><tr><td><i>pol-214</i></td><td>Polish (214).</td></tr><tr><td><i>pol-pr</i></td><td>Polish (Programmers).</td></tr><tr><td><i>pt</i></td><td>Portuguese.</td></tr><tr><td><i>pt-br</i></td><td>Portuguese (Brazilian ABNT).</td></tr><tr><td><i>pt-br-abnt2</i></td><td>Portuguese (Brazilian ABNT2).</td></tr><tr><td><i>ru</i></td><td>Russian.</td></tr><tr><td><i>ru-mne</i></td><td>Russian - Mnemonic.</td></tr><tr><td><i>ru-t</i></td><td>Russian (Typewriter).</td></tr><tr><td><i>sl</i></td><td>Slovenian.</td></tr><tr><td><i>sv</i></td><td>Swedish.</td></tr><tr><td><i>sv-sami</i></td><td>Swedish with Sami.</td></tr><tr><td><i>tuk</i></td><td>Turkmen.</td></tr><tr><td><i>tur-f</i></td><td>Turkish F.</td></tr><tr><td><i>tur-q</i></td><td>Turkish Q.</td></tr><tr><td><i>zh-sym-sg-us</i></td><td>Chinese (Simplified, Singapore) - US keyboard.</td></tr><tr><td><i>zh-sym-us</i></td><td>Chinese (Simplified) - US Keyboard.</td></tr><tr><td><i>zh-tr-hk</i></td><td>Chinese (Traditional, Hong Kong S.A.R.).</td></tr><tr><td><i>zh-tr-mo</i></td><td>Chinese (Traditional Macao S.A.R.) - US Keyboard.</td></tr><tr><td><i>zh-tr-us</i></td><td>Chinese (Traditional) - US keyboard.</td></tr></table>	Option	Description	<i>lt-std</i>	Lithuanian Standard.	<i>lav-std</i>	Latvian (Standard).	<i>lav-leg</i>	Latvian (Legacy).	<i>mk</i>	Macedonian (FYROM).	<i>mk-std</i>	Macedonia (FYROM) - Standard.	<i>no</i>	Norwegian.	<i>no-sami</i>	Norwegian with Sami.	<i>pol-214</i>	Polish (214).	<i>pol-pr</i>	Polish (Programmers).	<i>pt</i>	Portuguese.	<i>pt-br</i>	Portuguese (Brazilian ABNT).	<i>pt-br-abnt2</i>	Portuguese (Brazilian ABNT2).	<i>ru</i>	Russian.	<i>ru-mne</i>	Russian - Mnemonic.	<i>ru-t</i>	Russian (Typewriter).	<i>sl</i>	Slovenian.	<i>sv</i>	Swedish.	<i>sv-sami</i>	Swedish with Sami.	<i>tuk</i>	Turkmen.	<i>tur-f</i>	Turkish F.	<i>tur-q</i>	Turkish Q.	<i>zh-sym-sg-us</i>	Chinese (Simplified, Singapore) - US keyboard.	<i>zh-sym-us</i>	Chinese (Simplified) - US Keyboard.	<i>zh-tr-hk</i>	Chinese (Traditional, Hong Kong S.A.R.).	<i>zh-tr-mo</i>	Chinese (Traditional Macao S.A.R.) - US Keyboard.	<i>zh-tr-us</i>	Chinese (Traditional) - US keyboard.			
	Option	Description																																																								
	<i>lt-std</i>	Lithuanian Standard.																																																								
	<i>lav-std</i>	Latvian (Standard).																																																								
	<i>lav-leg</i>	Latvian (Legacy).																																																								
	<i>mk</i>	Macedonian (FYROM).																																																								
	<i>mk-std</i>	Macedonia (FYROM) - Standard.																																																								
	<i>no</i>	Norwegian.																																																								
	<i>no-sami</i>	Norwegian with Sami.																																																								
	<i>pol-214</i>	Polish (214).																																																								
	<i>pol-pr</i>	Polish (Programmers).																																																								
	<i>pt</i>	Portuguese.																																																								
	<i>pt-br</i>	Portuguese (Brazilian ABNT).																																																								
	<i>pt-br-abnt2</i>	Portuguese (Brazilian ABNT2).																																																								
	<i>ru</i>	Russian.																																																								
	<i>ru-mne</i>	Russian - Mnemonic.																																																								
	<i>ru-t</i>	Russian (Typewriter).																																																								
	<i>sl</i>	Slovenian.																																																								
	<i>sv</i>	Swedish.																																																								
	<i>sv-sami</i>	Swedish with Sami.																																																								
	<i>tuk</i>	Turkmen.																																																								
	<i>tur-f</i>	Turkish F.																																																								
	<i>tur-q</i>	Turkish Q.																																																								
	<i>zh-sym-sg-us</i>	Chinese (Simplified, Singapore) - US keyboard.																																																								
	<i>zh-sym-us</i>	Chinese (Simplified) - US Keyboard.																																																								
	<i>zh-tr-hk</i>	Chinese (Traditional, Hong Kong S.A.R.).																																																								
	<i>zh-tr-mo</i>	Chinese (Traditional Macao S.A.R.) - US Keyboard.																																																								
	<i>zh-tr-us</i>	Chinese (Traditional) - US keyboard.																																																								
security	Security mode for RDP connection.	option	-	rdp																																																						

Parameter	Description	Type	Size	Default										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>any</i></td><td>Allow the server to choose the type of security.</td></tr><tr><td><i>rdp</i></td><td>Standard RDP encryption.</td></tr><tr><td><i>nla</i></td><td>Network Level Authentication.</td></tr><tr><td><i>tls</i></td><td>TLS encryption.</td></tr></table>	Option	Description	<i>any</i>	Allow the server to choose the type of security.	<i>rdp</i>	Standard RDP encryption.	<i>nla</i>	Network Level Authentication.	<i>tls</i>	TLS encryption.			
	Option	Description												
	<i>any</i>	Allow the server to choose the type of security.												
	<i>rdp</i>	Standard RDP encryption.												
	<i>nla</i>	Network Level Authentication.												
<i>tls</i>	TLS encryption.													
send-preconnection-id	Enable/disable sending of preconnection ID.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable sending of preconnection ID.</td></tr><tr><td><i>disable</i></td><td>Disable sending of preconnection ID.</td></tr></table>	Option	Description	<i>enable</i>	Enable sending of preconnection ID.	<i>disable</i>	Disable sending of preconnection ID.							
	Option	Description												
	<i>enable</i>	Enable sending of preconnection ID.												
<i>disable</i>	Disable sending of preconnection ID.													
preconnection-id	The numeric ID of the RDP source.	integer	Minimum value: 0 Maximum value: 4294967295	0										
preconnection-blob	An arbitrary string which identifies the RDP source.	var-string	Maximum length: 511											
load-balancing-info	The load balancing information or cookie which should be provided to the connection broker.	var-string	Maximum length: 511											
restricted-admin	Enable/disable restricted admin mode for RDP.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable restricted admin mode for RDP.</td></tr><tr><td><i>disable</i></td><td>Disable restricted admin mode for RDP.</td></tr></table>	Option	Description	<i>enable</i>	Enable restricted admin mode for RDP.	<i>disable</i>	Disable restricted admin mode for RDP.							
	Option	Description												
	<i>enable</i>	Enable restricted admin mode for RDP.												
<i>disable</i>	Disable restricted admin mode for RDP.													
port	Remote port.	integer	Minimum value: 0 Maximum value: 65535	0										
logon-user	Logon user.	var-string	Maximum length: 35											
logon-password	Logon password.	password	Not Specified											
color-depth	Color depth per pixel.	option	-	16										

Parameter	Description	Type	Size	Default
	<div><div>Option</div><div>Description</div></div>			
	32	32bits per pixel.		
	16	16bits per pixel.		
	8	8bits per pixel.		
sso	Single Sign-On.	option	-	disable
	<div><div>Option</div><div>Description</div></div>			
	disable	Disable SSO.		
	static	Static SSO.		
	auto	Auto SSO.		
sso-credential	Single sign-on credentials.	option	-	sslvpn-login
	<div><div>Option</div><div>Description</div></div>			
	sslvpn-login	SSL-VPN login.		
	alternative	Alternative.		
sso-username	SSO user name.	var-string	Maximum length: 35	
sso-password	SSO password.	password	Not Specified	
sso-credential-sent-once	Single sign-on credentials are only sent once to remote server.	option	-	disable
	<div><div>Option</div><div>Description</div></div>			
	enable	Single sign-on credentials are only sent once to remote server.		
	disable	Single sign-on credentials are sent to remote server for every HTTP request.		
width	Screen width.	integer	Minimum value: 0 Maximum value: 65535	0
height	Screen height.	integer	Minimum value: 0 Maximum value: 65535	0

## config form-data

Parameter	Description	Type	Size	Default
name	Name.	string	Maximum length: 35	
value	Value.	var-string	Maximum length: 63	

## config mac-addr-check-rule

Parameter	Description	Type	Size	Default
name	Client MAC address check rule name.	string	Maximum length: 35	
mac-addr-mask	Client MAC address mask.	integer	Minimum value: 1 Maximum value: 48	48
mac-addr-list <addr>	Client MAC address list. Client MAC address.	mac-address	Not Specified	

## config os-check-list

Parameter	Description	Type	Size	Default								
name	Name.	string	Maximum length: 35									
action	OS check options.	option	-	allow								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>deny</i></td><td>Deny all OS versions.</td></tr><tr><td><i>allow</i></td><td>Allow any OS version.</td></tr><tr><td><i>check-up-to-date</i></td><td>Verify OS is up-to-date.</td></tr></table>				Option	Description	<i>deny</i>	Deny all OS versions.	<i>allow</i>	Allow any OS version.	<i>check-up-to-date</i>	Verify OS is up-to-date.
	Option	Description										
	<i>deny</i>	Deny all OS versions.										
	<i>allow</i>	Allow any OS version.										
<i>check-up-to-date</i>	Verify OS is up-to-date.											
tolerance	OS patch level tolerance.	integer	Minimum value: 0 Maximum value: 65535	0								
latest-patch-level	Latest OS patch level.	user	Not Specified	0								

## config split-dns

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967294	0
domains	Split DNS domains used for SSL-VPN clients separated by comma.	var-string	Maximum length: 1024	
dns-server1	DNS server 1.	ipv4-address	Not Specified	0.0.0.0
dns-server2	DNS server 2.	ipv4-address	Not Specified	0.0.0.0
ipv6-dns-server1	IPv6 DNS server 1.	ipv6-address	Not Specified	::
ipv6-dns-server2	IPv6 DNS server 2.	ipv6-address	Not Specified	::

## config vpn ssl web realm

Realm.

```
config vpn ssl web realm
  Description: Realm.
  edit <url-path>
    set login-page {var-string}
    set max-concurrent-user {integer}
    set nas-ip {ipv4-address}
    set radius-port {integer}
    set radius-server {string}
    set virtual-host {var-string}
    set virtual-host-only [enable|disable]
    set virtual-host-server-cert {string}
  next
end
```

## config vpn ssl web realm

Parameter	Description	Type	Size	Default
login-page	Replacement HTML for SSL-VPN login page.	var-string	Maximum length: 32768	

Parameter	Description	Type	Size	Default
max-concurrent-user	Maximum concurrent users.	integer	Minimum value: 0 Maximum value: 65535	0
nas-ip	IP address used as a NAS-IP to communicate with the RADIUS server.	ipv4-address	Not Specified	0.0.0.0
radius-port	RADIUS service port number.	integer	Minimum value: 0 Maximum value: 65535	0
radius-server	RADIUS server associated with realm.	string	Maximum length: 35	
url-path	URL path to access SSL-VPN login page.	string	Maximum length: 35	
virtual-host	Virtual host name for realm.	var-string	Maximum length: 255	
virtual-host-only	Enable/disable enforcement of virtual host method for SSL-VPN client access.	option	-	disable
	Option	Description		
	enable	Enable setting.		
	disable	Disable setting.		
virtual-host-server-cert	Name of the server certificate to used for this realm.	string	Maximum length: 35	

## config vpn ssl web user-bookmark

Configure SSL-VPN user bookmark.

```

config vpn ssl web user-bookmark
  Description: Configure SSL-VPN user bookmark.
  edit <name>
    config bookmarks
      Description: Bookmark table.
      edit <name>
        set apptype [ftp|rdp|...]
        set url {var-string}
        set host {var-string}
        set folder {var-string}
        set domain {var-string}
        set additional-params {var-string}
        set description {var-string}

```

```

    set keyboard-layout [ar-101|ar-102|...]
    set security [any|rdp|...]
    set send-preconnection-id [enable|disable]
    set preconnection-id {integer}
    set preconnection-blob {var-string}
    set load-balancing-info {var-string}
    set restricted-admin [enable|disable]
    set port {integer}
    set logon-user {var-string}
    set logon-password {password}
    set color-depth [32|16|...]
    set sso [disable|static|...]
    config form-data
        Description: Form data.
        edit <name>
            set value {var-string}
        next
    end
    set sso-credential [sslvpn-login|alternative]
    set sso-username {var-string}
    set sso-password {password}
    set sso-credential-sent-once [enable|disable]
    set width {integer}
    set height {integer}
next
end
    set custom-lang {string}
next
end

```

## config vpn ssl web user-bookmark

Parameter	Description	Type	Size	Default
custom-lang	Personal language.	string	Maximum length: 35	
name	User and group name.	string	Maximum length: 101	

## config bookmarks

Parameter	Description	Type	Size	Default
name	Bookmark name.	string	Maximum length: 35	
apptype	Application type.	option	-	web
	<b>Option</b>	<b>Description</b>		
	<i>ftp</i>	FTP.		



Parameter	Description	Type	Size	Default																					
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>rdp</i></td><td>RDP.</td></tr><tr><td><i>sftp</i></td><td>SFTP.</td></tr><tr><td><i>smb</i></td><td>SMB/CIFS.</td></tr><tr><td><i>ssh</i></td><td>SSH.</td></tr><tr><td><i>telnet</i></td><td>Telnet.</td></tr><tr><td><i>vnc</i></td><td>VNC.</td></tr><tr><td><i>web</i></td><td>HTTP/HTTPS.</td></tr></table>		Option	Description	<i>rdp</i>	RDP.	<i>sftp</i>	SFTP.	<i>smb</i>	SMB/CIFS.	<i>ssh</i>	SSH.	<i>telnet</i>	Telnet.	<i>vnc</i>	VNC.	<i>web</i>	HTTP/HTTPS.							
	Option	Description																							
	<i>rdp</i>	RDP.																							
	<i>sftp</i>	SFTP.																							
	<i>smb</i>	SMB/CIFS.																							
	<i>ssh</i>	SSH.																							
	<i>telnet</i>	Telnet.																							
	<i>vnc</i>	VNC.																							
<i>web</i>	HTTP/HTTPS.																								
url	URL parameter.	var-string	Maximum length: 128																						
host	Host name/IP parameter.	var-string	Maximum length: 128																						
folder	Network shared file folder parameter.	var-string	Maximum length: 128																						
domain	Login domain.	var-string	Maximum length: 128																						
additional-params	Additional parameters.	var-string	Maximum length: 128																						
description	Description.	var-string	Maximum length: 128																						
keyboard-layout	Keyboard layout.	option	-	en-us																					
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ar-101</i></td><td>Arabic (101).</td></tr><tr><td><i>ar-102</i></td><td>Arabic (102).</td></tr><tr><td><i>ar-102-azerty</i></td><td>Arabic (102) AZERTY.</td></tr><tr><td><i>can-mul</i></td><td>Canadian Multilingual Standard.</td></tr><tr><td><i>cz</i></td><td>Czech.</td></tr><tr><td><i>cz-qwerty</i></td><td>Czech (QWERTY).</td></tr><tr><td><i>cz-pr</i></td><td>Czech Programmers.</td></tr><tr><td><i>da</i></td><td>Danish.</td></tr><tr><td><i>nl</i></td><td>Dutch.</td></tr></table>		Option	Description	<i>ar-101</i>	Arabic (101).	<i>ar-102</i>	Arabic (102).	<i>ar-102-azerty</i>	Arabic (102) AZERTY.	<i>can-mul</i>	Canadian Multilingual Standard.	<i>cz</i>	Czech.	<i>cz-qwerty</i>	Czech (QWERTY).	<i>cz-pr</i>	Czech Programmers.	<i>da</i>	Danish.	<i>nl</i>	Dutch.			
	Option	Description																							
	<i>ar-101</i>	Arabic (101).																							
	<i>ar-102</i>	Arabic (102).																							
	<i>ar-102-azerty</i>	Arabic (102) AZERTY.																							
	<i>can-mul</i>	Canadian Multilingual Standard.																							
	<i>cz</i>	Czech.																							
	<i>cz-qwerty</i>	Czech (QWERTY).																							
	<i>cz-pr</i>	Czech Programmers.																							
	<i>da</i>	Danish.																							
<i>nl</i>	Dutch.																								

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>de</i>	German.		
	<i>de-ch</i>	German, Switzerland.		
	<i>de-ibm</i>	German (IBM).		
	<i>en-uk</i>	English, United Kingdom.		
	<i>en-uk-ext</i>	English, United Kingdom Extended.		
	<i>en-us</i>	English, United States.		
	<i>en-us-dvorak</i>	English, United States-Dvorak.		
	<i>es</i>	Spanish.		
	<i>es-var</i>	Spanish Variation.		
	<i>fi</i>	Finnish.		
	<i>fi-sami</i>	Finnish with Sami.		
	<i>fr</i>	French.		
	<i>fr-apple</i>	French, Apple.		
	<i>fr-ca</i>	French, Canada.		
	<i>fr-ch</i>	French, Switzerland.		
	<i>fr-be</i>	French, Belgium.		
	<i>hr</i>	Croatian.		
	<i>hu</i>	Hungarian.		
	<i>hu-101</i>	Hungarian 101-Key.		
	<i>it</i>	Italian.		
	<i>it-142</i>	Italian (142).		
	<i>ja</i>	Japanese.		
	<i>ko</i>	Korean.		
	<i>lt</i>	Lithuanian.		
	<i>lt-ibm</i>	Lithuanian IBM.		
	<i>lt-std</i>	Lithuanian Standard.		
	<i>lav-std</i>	Latvian (Standard).		
	<i>lav-leg</i>	Latvian (Legacy).		
	<i>mk</i>	Macedonian (FYROM).		

Parameter	Description	Type	Size	Default																																														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>mk-std</i></td><td>Macedonia (FYROM) - Standard.</td></tr><tr><td><i>no</i></td><td>Norwegian.</td></tr><tr><td><i>no-sami</i></td><td>Norwegian with Sami.</td></tr><tr><td><i>pol-214</i></td><td>Polish (214).</td></tr><tr><td><i>pol-pr</i></td><td>Polish (Programmers).</td></tr><tr><td><i>pt</i></td><td>Portuguese.</td></tr><tr><td><i>pt-br</i></td><td>Portuguese (Brazilian ABNT).</td></tr><tr><td><i>pt-br-abnt2</i></td><td>Portuguese (Brazilian ABNT2).</td></tr><tr><td><i>ru</i></td><td>Russian.</td></tr><tr><td><i>ru-mne</i></td><td>Russian - Mnemonic.</td></tr><tr><td><i>ru-t</i></td><td>Russian (Typewriter).</td></tr><tr><td><i>sl</i></td><td>Slovenian.</td></tr><tr><td><i>sv</i></td><td>Swedish.</td></tr><tr><td><i>sv-sami</i></td><td>Swedish with Sami.</td></tr><tr><td><i>tuk</i></td><td>Turkmen.</td></tr><tr><td><i>tur-f</i></td><td>Turkish F.</td></tr><tr><td><i>tur-q</i></td><td>Turkish Q.</td></tr><tr><td><i>zh-sym-sg-us</i></td><td>Chinese (Simplified, Singapore) - US keyboard.</td></tr><tr><td><i>zh-sym-us</i></td><td>Chinese (Simplified) - US Keyboard.</td></tr><tr><td><i>zh-tr-hk</i></td><td>Chinese (Traditional, Hong Kong S.A.R.).</td></tr><tr><td><i>zh-tr-mo</i></td><td>Chinese (Traditional Macao S.A.R.) - US Keyboard.</td></tr><tr><td><i>zh-tr-us</i></td><td>Chinese (Traditional) - US keyboard.</td></tr></table>	Option	Description	<i>mk-std</i>	Macedonia (FYROM) - Standard.	<i>no</i>	Norwegian.	<i>no-sami</i>	Norwegian with Sami.	<i>pol-214</i>	Polish (214).	<i>pol-pr</i>	Polish (Programmers).	<i>pt</i>	Portuguese.	<i>pt-br</i>	Portuguese (Brazilian ABNT).	<i>pt-br-abnt2</i>	Portuguese (Brazilian ABNT2).	<i>ru</i>	Russian.	<i>ru-mne</i>	Russian - Mnemonic.	<i>ru-t</i>	Russian (Typewriter).	<i>sl</i>	Slovenian.	<i>sv</i>	Swedish.	<i>sv-sami</i>	Swedish with Sami.	<i>tuk</i>	Turkmen.	<i>tur-f</i>	Turkish F.	<i>tur-q</i>	Turkish Q.	<i>zh-sym-sg-us</i>	Chinese (Simplified, Singapore) - US keyboard.	<i>zh-sym-us</i>	Chinese (Simplified) - US Keyboard.	<i>zh-tr-hk</i>	Chinese (Traditional, Hong Kong S.A.R.).	<i>zh-tr-mo</i>	Chinese (Traditional Macao S.A.R.) - US Keyboard.	<i>zh-tr-us</i>	Chinese (Traditional) - US keyboard.			
	Option	Description																																																
	<i>mk-std</i>	Macedonia (FYROM) - Standard.																																																
	<i>no</i>	Norwegian.																																																
	<i>no-sami</i>	Norwegian with Sami.																																																
	<i>pol-214</i>	Polish (214).																																																
	<i>pol-pr</i>	Polish (Programmers).																																																
	<i>pt</i>	Portuguese.																																																
	<i>pt-br</i>	Portuguese (Brazilian ABNT).																																																
	<i>pt-br-abnt2</i>	Portuguese (Brazilian ABNT2).																																																
	<i>ru</i>	Russian.																																																
	<i>ru-mne</i>	Russian - Mnemonic.																																																
	<i>ru-t</i>	Russian (Typewriter).																																																
	<i>sl</i>	Slovenian.																																																
	<i>sv</i>	Swedish.																																																
	<i>sv-sami</i>	Swedish with Sami.																																																
	<i>tuk</i>	Turkmen.																																																
	<i>tur-f</i>	Turkish F.																																																
	<i>tur-q</i>	Turkish Q.																																																
	<i>zh-sym-sg-us</i>	Chinese (Simplified, Singapore) - US keyboard.																																																
	<i>zh-sym-us</i>	Chinese (Simplified) - US Keyboard.																																																
	<i>zh-tr-hk</i>	Chinese (Traditional, Hong Kong S.A.R.).																																																
<i>zh-tr-mo</i>	Chinese (Traditional Macao S.A.R.) - US Keyboard.																																																	
<i>zh-tr-us</i>	Chinese (Traditional) - US keyboard.																																																	
security	Security mode for RDP connection.	option	-	rdp																																														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>any</i></td><td>Allow the server to choose the type of security.</td></tr><tr><td><i>rdp</i></td><td>Standard RDP encryption.</td></tr><tr><td><i>nla</i></td><td>Network Level Authentication.</td></tr><tr><td><i>tls</i></td><td>TLS encryption.</td></tr></table>	Option	Description	<i>any</i>	Allow the server to choose the type of security.	<i>rdp</i>	Standard RDP encryption.	<i>nla</i>	Network Level Authentication.	<i>tls</i>	TLS encryption.																																							
	Option	Description																																																
	<i>any</i>	Allow the server to choose the type of security.																																																
	<i>rdp</i>	Standard RDP encryption.																																																
	<i>nla</i>	Network Level Authentication.																																																
<i>tls</i>	TLS encryption.																																																	

Parameter	Description	Type	Size	Default
send-preconnection-id	Enable/disable sending of preconnection ID.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable sending of preconnection ID.		
	<i>disable</i>	Disable sending of preconnection ID.		
preconnection-id	The numeric ID of the RDP source.	integer	Minimum value: 0 Maximum value: 4294967295	0
preconnection-blob	An arbitrary string which identifies the RDP source.	var-string	Maximum length: 511	
load-balancing-info	The load balancing information or cookie which should be provided to the connection broker.	var-string	Maximum length: 511	
restricted-admin	Enable/disable restricted admin mode for RDP.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable restricted admin mode for RDP.		
	<i>disable</i>	Disable restricted admin mode for RDP.		
port	Remote port.	integer	Minimum value: 0 Maximum value: 65535	0
logon-user	Logon user.	var-string	Maximum length: 35	
logon-password	Logon password.	password	Not Specified	
color-depth	Color depth per pixel.	option	-	16
	<b>Option</b>	<b>Description</b>		
	32	32bits per pixel.		
	16	16bits per pixel.		
	8	8bits per pixel.		
sso	Single Sign-On.	option	-	disable

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable SSO.</td></tr><tr><td><i>static</i></td><td>Static SSO.</td></tr><tr><td><i>auto</i></td><td>Auto SSO.</td></tr></table>				Option	Description	<i>disable</i>	Disable SSO.	<i>static</i>	Static SSO.	<i>auto</i>	Auto SSO.
	Option	Description										
	<i>disable</i>	Disable SSO.										
	<i>static</i>	Static SSO.										
<i>auto</i>	Auto SSO.											
sso-credential	Single sign-on credentials.	option	-	sslvpn-login								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>sslvpn-login</i></td><td>SSL-VPN login.</td></tr><tr><td><i>alternative</i></td><td>Alternative.</td></tr></table>				Option	Description	<i>sslvpn-login</i>	SSL-VPN login.	<i>alternative</i>	Alternative.		
	Option	Description										
	<i>sslvpn-login</i>	SSL-VPN login.										
<i>alternative</i>	Alternative.											
sso-username	SSO user name.	var-string	Maximum length: 35									
sso-password	SSO password.	password	Not Specified									
sso-credential-sent-once	Single sign-on credentials are only sent once to remote server.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Single sign-on credentials are only sent once to remote server.</td></tr><tr><td><i>disable</i></td><td>Single sign-on credentials are sent to remote server for every HTTP request.</td></tr></table>				Option	Description	<i>enable</i>	Single sign-on credentials are only sent once to remote server.	<i>disable</i>	Single sign-on credentials are sent to remote server for every HTTP request.		
	Option	Description										
	<i>enable</i>	Single sign-on credentials are only sent once to remote server.										
<i>disable</i>	Single sign-on credentials are sent to remote server for every HTTP request.											
width	Screen width.	integer	Minimum value: 0 Maximum value: 65535	0								
height	Screen height.	integer	Minimum value: 0 Maximum value: 65535	0								

#### config form-data

Parameter	Description	Type	Size	Default
name	Name.	string	Maximum length: 35	
value	Value.	var-string	Maximum length: 63	

## config vpn ssl web user-group-bookmark

Configure SSL-VPN user group bookmark.

```
config vpn ssl web user-group-bookmark
  Description: Configure SSL-VPN user group bookmark.
  edit <name>
    config bookmarks
      Description: Bookmark table.
      edit <name>
        set apptype [ftp|rdp|...]
        set url {var-string}
        set host {var-string}
        set folder {var-string}
        set domain {var-string}
        set additional-params {var-string}
        set description {var-string}
        set keyboard-layout [ar-101|ar-102|...]
        set security [any|rdp|...]
        set send-preconnection-id [enable|disable]
        set preconnection-id {integer}
        set preconnection-blob {var-string}
        set load-balancing-info {var-string}
        set restricted-admin [enable|disable]
        set port {integer}
        set logon-user {var-string}
        set logon-password {password}
        set color-depth [32|16|...]
        set sso [disable|static|...]
        config form-data
          Description: Form data.
          edit <name>
            set value {var-string}
          next
        end
        set sso-credential [sslvpn-login|alternative]
        set sso-username {var-string}
        set sso-password {password}
        set sso-credential-sent-once [enable|disable]
        set width {integer}
        set height {integer}
      next
    end
  next
end
```

## config vpn ssl web user-group-bookmark

Parameter	Description	Type	Size	Default
name	Group name.	string	Maximum length: 64	

## config bookmarks

Parameter	Description	Type	Size	Default
name	Bookmark name.	string	Maximum length: 35	
apptype	Application type.	option	-	web
	<b>Option</b>	<b>Description</b>		
	<i>ftp</i>	FTP.		
	<i>rdp</i>	RDP.		
	<i>sftp</i>	SFTP.		
	<i>smb</i>	SMB/CIFS.		
	<i>ssh</i>	SSH.		
	<i>telnet</i>	Telnet.		
	<i>vnc</i>	VNC.		
	<i>web</i>	HTTP/HTTPS.		
url	URL parameter.	var-string	Maximum length: 128	
host	Host name/IP parameter.	var-string	Maximum length: 128	
folder	Network shared file folder parameter.	var-string	Maximum length: 128	
domain	Login domain.	var-string	Maximum length: 128	
additional-params	Additional parameters.	var-string	Maximum length: 128	
description	Description.	var-string	Maximum length: 128	
keyboard-layout	Keyboard layout.	option	-	en-us
	<b>Option</b>	<b>Description</b>		
	<i>ar-101</i>	Arabic (101).		
	<i>ar-102</i>	Arabic (102).		
	<i>ar-102-azerty</i>	Arabic (102) AZERTY.		
	<i>can-mul</i>	Canadian Multilingual Standard.		
	<i>cz</i>	Czech.		

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>cz-qwerty</i>	Czech (QWERTY).		
	<i>cz-pr</i>	Czech Programmers.		
	<i>da</i>	Danish.		
	<i>nl</i>	Dutch.		
	<i>de</i>	German.		
	<i>de-ch</i>	German, Switzerland.		
	<i>de-ibm</i>	German (IBM).		
	<i>en-uk</i>	English, United Kingdom.		
	<i>en-uk-ext</i>	English, United Kingdom Extended.		
	<i>en-us</i>	English, United States.		
	<i>en-us-dvorak</i>	English, United States-Dvorak.		
	<i>es</i>	Spanish.		
	<i>es-var</i>	Spanish Variation.		
	<i>fi</i>	Finnish.		
	<i>fi-sami</i>	Finnish with Sami.		
	<i>fr</i>	French.		
	<i>fr-apple</i>	French, Apple.		
	<i>fr-ca</i>	French, Canada.		
	<i>fr-ch</i>	French, Switzerland.		
	<i>fr-be</i>	French, Belgium.		
	<i>hr</i>	Croatian.		
	<i>hu</i>	Hungarian.		
	<i>hu-101</i>	Hungarian 101-Key.		
	<i>it</i>	Italian.		
	<i>it-142</i>	Italian (142).		
	<i>ja</i>	Japanese.		
	<i>ko</i>	Korean.		
	<i>lt</i>	Lithuanian.		
	<i>lt-ibm</i>	Lithuanian IBM.		



Parameter	Description	Type	Size	Default																																																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>lt-std</i></td><td>Lithuanian Standard.</td></tr><tr><td><i>lav-std</i></td><td>Latvian (Standard).</td></tr><tr><td><i>lav-leg</i></td><td>Latvian (Legacy).</td></tr><tr><td><i>mk</i></td><td>Macedonian (FYROM).</td></tr><tr><td><i>mk-std</i></td><td>Macedonia (FYROM) - Standard.</td></tr><tr><td><i>no</i></td><td>Norwegian.</td></tr><tr><td><i>no-sami</i></td><td>Norwegian with Sami.</td></tr><tr><td><i>pol-214</i></td><td>Polish (214).</td></tr><tr><td><i>pol-pr</i></td><td>Polish (Programmers).</td></tr><tr><td><i>pt</i></td><td>Portuguese.</td></tr><tr><td><i>pt-br</i></td><td>Portuguese (Brazilian ABNT).</td></tr><tr><td><i>pt-br-abnt2</i></td><td>Portuguese (Brazilian ABNT2).</td></tr><tr><td><i>ru</i></td><td>Russian.</td></tr><tr><td><i>ru-mne</i></td><td>Russian - Mnemonic.</td></tr><tr><td><i>ru-t</i></td><td>Russian (Typewriter).</td></tr><tr><td><i>sl</i></td><td>Slovenian.</td></tr><tr><td><i>sv</i></td><td>Swedish.</td></tr><tr><td><i>sv-sami</i></td><td>Swedish with Sami.</td></tr><tr><td><i>tuk</i></td><td>Turkmen.</td></tr><tr><td><i>tur-f</i></td><td>Turkish F.</td></tr><tr><td><i>tur-q</i></td><td>Turkish Q.</td></tr><tr><td><i>zh-sym-sg-us</i></td><td>Chinese (Simplified, Singapore) - US keyboard.</td></tr><tr><td><i>zh-sym-us</i></td><td>Chinese (Simplified) - US Keyboard.</td></tr><tr><td><i>zh-tr-hk</i></td><td>Chinese (Traditional, Hong Kong S.A.R.).</td></tr><tr><td><i>zh-tr-mo</i></td><td>Chinese (Traditional Macao S.A.R.) - US Keyboard.</td></tr><tr><td><i>zh-tr-us</i></td><td>Chinese (Traditional) - US keyboard.</td></tr></table>	Option	Description	<i>lt-std</i>	Lithuanian Standard.	<i>lav-std</i>	Latvian (Standard).	<i>lav-leg</i>	Latvian (Legacy).	<i>mk</i>	Macedonian (FYROM).	<i>mk-std</i>	Macedonia (FYROM) - Standard.	<i>no</i>	Norwegian.	<i>no-sami</i>	Norwegian with Sami.	<i>pol-214</i>	Polish (214).	<i>pol-pr</i>	Polish (Programmers).	<i>pt</i>	Portuguese.	<i>pt-br</i>	Portuguese (Brazilian ABNT).	<i>pt-br-abnt2</i>	Portuguese (Brazilian ABNT2).	<i>ru</i>	Russian.	<i>ru-mne</i>	Russian - Mnemonic.	<i>ru-t</i>	Russian (Typewriter).	<i>sl</i>	Slovenian.	<i>sv</i>	Swedish.	<i>sv-sami</i>	Swedish with Sami.	<i>tuk</i>	Turkmen.	<i>tur-f</i>	Turkish F.	<i>tur-q</i>	Turkish Q.	<i>zh-sym-sg-us</i>	Chinese (Simplified, Singapore) - US keyboard.	<i>zh-sym-us</i>	Chinese (Simplified) - US Keyboard.	<i>zh-tr-hk</i>	Chinese (Traditional, Hong Kong S.A.R.).	<i>zh-tr-mo</i>	Chinese (Traditional Macao S.A.R.) - US Keyboard.	<i>zh-tr-us</i>	Chinese (Traditional) - US keyboard.			
	Option	Description																																																								
	<i>lt-std</i>	Lithuanian Standard.																																																								
	<i>lav-std</i>	Latvian (Standard).																																																								
	<i>lav-leg</i>	Latvian (Legacy).																																																								
	<i>mk</i>	Macedonian (FYROM).																																																								
	<i>mk-std</i>	Macedonia (FYROM) - Standard.																																																								
	<i>no</i>	Norwegian.																																																								
	<i>no-sami</i>	Norwegian with Sami.																																																								
	<i>pol-214</i>	Polish (214).																																																								
	<i>pol-pr</i>	Polish (Programmers).																																																								
	<i>pt</i>	Portuguese.																																																								
	<i>pt-br</i>	Portuguese (Brazilian ABNT).																																																								
	<i>pt-br-abnt2</i>	Portuguese (Brazilian ABNT2).																																																								
	<i>ru</i>	Russian.																																																								
	<i>ru-mne</i>	Russian - Mnemonic.																																																								
	<i>ru-t</i>	Russian (Typewriter).																																																								
	<i>sl</i>	Slovenian.																																																								
	<i>sv</i>	Swedish.																																																								
	<i>sv-sami</i>	Swedish with Sami.																																																								
	<i>tuk</i>	Turkmen.																																																								
	<i>tur-f</i>	Turkish F.																																																								
	<i>tur-q</i>	Turkish Q.																																																								
	<i>zh-sym-sg-us</i>	Chinese (Simplified, Singapore) - US keyboard.																																																								
	<i>zh-sym-us</i>	Chinese (Simplified) - US Keyboard.																																																								
	<i>zh-tr-hk</i>	Chinese (Traditional, Hong Kong S.A.R.).																																																								
	<i>zh-tr-mo</i>	Chinese (Traditional Macao S.A.R.) - US Keyboard.																																																								
	<i>zh-tr-us</i>	Chinese (Traditional) - US keyboard.																																																								
security	Security mode for RDP connection.	option	-	rdp																																																						

Parameter	Description	Type	Size	Default										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>any</i></td><td>Allow the server to choose the type of security.</td></tr><tr><td><i>rdp</i></td><td>Standard RDP encryption.</td></tr><tr><td><i>nla</i></td><td>Network Level Authentication.</td></tr><tr><td><i>tls</i></td><td>TLS encryption.</td></tr></table>	Option	Description	<i>any</i>	Allow the server to choose the type of security.	<i>rdp</i>	Standard RDP encryption.	<i>nla</i>	Network Level Authentication.	<i>tls</i>	TLS encryption.			
	Option	Description												
	<i>any</i>	Allow the server to choose the type of security.												
	<i>rdp</i>	Standard RDP encryption.												
	<i>nla</i>	Network Level Authentication.												
<i>tls</i>	TLS encryption.													
send-preconnection-id	Enable/disable sending of preconnection ID.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable sending of preconnection ID.</td></tr><tr><td><i>disable</i></td><td>Disable sending of preconnection ID.</td></tr></table>	Option	Description	<i>enable</i>	Enable sending of preconnection ID.	<i>disable</i>	Disable sending of preconnection ID.							
	Option	Description												
	<i>enable</i>	Enable sending of preconnection ID.												
<i>disable</i>	Disable sending of preconnection ID.													
preconnection-id	The numeric ID of the RDP source.	integer	Minimum value: 0 Maximum value: 4294967295	0										
preconnection-blob	An arbitrary string which identifies the RDP source.	var-string	Maximum length: 511											
load-balancing-info	The load balancing information or cookie which should be provided to the connection broker.	var-string	Maximum length: 511											
restricted-admin	Enable/disable restricted admin mode for RDP.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable restricted admin mode for RDP.</td></tr><tr><td><i>disable</i></td><td>Disable restricted admin mode for RDP.</td></tr></table>	Option	Description	<i>enable</i>	Enable restricted admin mode for RDP.	<i>disable</i>	Disable restricted admin mode for RDP.							
	Option	Description												
	<i>enable</i>	Enable restricted admin mode for RDP.												
<i>disable</i>	Disable restricted admin mode for RDP.													
port	Remote port.	integer	Minimum value: 0 Maximum value: 65535	0										
logon-user	Logon user.	var-string	Maximum length: 35											
logon-password	Logon password.	password	Not Specified											
color-depth	Color depth per pixel.	option	-	16										

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>32</td><td>32bits per pixel.</td></tr><tr><td>16</td><td>16bits per pixel.</td></tr><tr><td>8</td><td>8bits per pixel.</td></tr></table>				Option	Description	32	32bits per pixel.	16	16bits per pixel.	8	8bits per pixel.
	Option	Description										
	32	32bits per pixel.										
	16	16bits per pixel.										
	8	8bits per pixel.										
sso	Single Sign-On.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable SSO.</td></tr><tr><td>static</td><td>Static SSO.</td></tr><tr><td>auto</td><td>Auto SSO.</td></tr></table>				Option	Description	disable	Disable SSO.	static	Static SSO.	auto	Auto SSO.
	Option	Description										
	disable	Disable SSO.										
	static	Static SSO.										
auto	Auto SSO.											
sso-credential	Single sign-on credentials.	option	-	sslvpn-login								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>sslvpn-login</td><td>SSL-VPN login.</td></tr><tr><td>alternative</td><td>Alternative.</td></tr></table>				Option	Description	sslvpn-login	SSL-VPN login.	alternative	Alternative.		
	Option	Description										
	sslvpn-login	SSL-VPN login.										
alternative	Alternative.											
sso-username	SSO user name.	var-string	Maximum length: 35									
sso-password	SSO password.	password	Not Specified									
sso-credential-sent-once	Single sign-on credentials are only sent once to remote server.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Single sign-on credentials are only sent once to remote server.</td></tr><tr><td>disable</td><td>Single sign-on credentials are sent to remote server for every HTTP request.</td></tr></table>				Option	Description	enable	Single sign-on credentials are only sent once to remote server.	disable	Single sign-on credentials are sent to remote server for every HTTP request.		
	Option	Description										
	enable	Single sign-on credentials are only sent once to remote server.										
disable	Single sign-on credentials are sent to remote server for every HTTP request.											
width	Screen width.	integer	Minimum value: 0 Maximum value: 65535	0								
height	Screen height.	integer	Minimum value: 0 Maximum value: 65535	0								

---

**config form-data**

Parameter	Description	Type	Size	Default
name	Name.	string	Maximum length: 35	
value	Value.	var-string	Maximum length: 63	

## waf

This section includes syntax for the following commands:

- [config waf main-class on page 1801](#)
- [config waf profile on page 1801](#)
- [config waf signature on page 1826](#)
- [config waf sub-class on page 1827](#)

### config waf main-class

Hidden table for datasource.

```
config waf main-class
    Description: Hidden table for datasource.
    edit <id>
        set name {string}
    next
end
```

### config waf main-class

Parameter	Description	Type	Size	Default
id	Main signature class ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
name	Main signature class name.	string	Maximum length: 127	

### config waf profile

Configure Web application firewall configuration.

```
config waf profile
    Description: Configure Web application firewall configuration.
    edit <name>
        config address-list
            Description: Address block and allow lists.
            set status [enable|disable]
            set blocked-log [enable|disable]
            set severity [high|medium|...]
            set trusted-address <name1>, <name2>, ...
```

```

        set blocked-address <name1>, <name2>, ...
    end
    set comment {var-string}
    config constraint
        Description: WAF HTTP protocol restrictions.
        config header-length
            Description: HTTP header length in request.
            set status [enable|disable]
            set length {integer}
            set action [allow|block]
            set log [enable|disable]
            set severity [high|medium|...]
        end
        config content-length
            Description: HTTP content length in request.
            set status [enable|disable]
            set length {integer}
            set action [allow|block]
            set log [enable|disable]
            set severity [high|medium|...]
        end
        config param-length
            Description: Maximum length of parameter in URL, HTTP POST request or HTTP
body.
            set status [enable|disable]
            set length {integer}
            set action [allow|block]
            set log [enable|disable]
            set severity [high|medium|...]
        end
        config line-length
            Description: HTTP line length in request.
            set status [enable|disable]
            set length {integer}
            set action [allow|block]
            set log [enable|disable]
            set severity [high|medium|...]
        end
        config url-param-length
            Description: Maximum length of parameter in URL.
            set status [enable|disable]
            set length {integer}
            set action [allow|block]
            set log [enable|disable]
            set severity [high|medium|...]
        end
        config version
            Description: Enable/disable HTTP version check.
            set status [enable|disable]
            set action [allow|block]
            set log [enable|disable]
            set severity [high|medium|...]
        end
        config method
            Description: Enable/disable HTTP method check.
            set status [enable|disable]

```

```

        set action [allow|block]
        set log [enable|disable]
        set severity [high|medium|...]
    end
    config hostname
        Description: Enable/disable hostname check.
        set status [enable|disable]
        set action [allow|block]
        set log [enable|disable]
        set severity [high|medium|...]
    end
    config malformed
        Description: Enable/disable malformed HTTP request check.
        set status [enable|disable]
        set action [allow|block]
        set log [enable|disable]
        set severity [high|medium|...]
    end
    config max-cookie
        Description: Maximum number of cookies in HTTP request.
        set status [enable|disable]
        set max-cookie {integer}
        set action [allow|block]
        set log [enable|disable]
        set severity [high|medium|...]
    end
    config max-header-line
        Description: Maximum number of HTTP header line.
        set status [enable|disable]
        set max-header-line {integer}
        set action [allow|block]
        set log [enable|disable]
        set severity [high|medium|...]
    end
    config max-url-param
        Description: Maximum number of parameters in URL.
        set status [enable|disable]
        set max-url-param {integer}
        set action [allow|block]
        set log [enable|disable]
        set severity [high|medium|...]
    end
    config max-range-segment
        Description: Maximum number of range segments in HTTP range line.
        set status [enable|disable]
        set max-range-segment {integer}
        set action [allow|block]
        set log [enable|disable]
        set severity [high|medium|...]
    end
    config exception
        Description: HTTP constraint exception.
        edit <id>
            set pattern {string}
            set regex [enable|disable]
            set address {string}

```

```

        set header-length [enable|disable]
        set content-length [enable|disable]
        set param-length [enable|disable]
        set line-length [enable|disable]
        set url-param-length [enable|disable]
        set version [enable|disable]
        set method [enable|disable]
        set hostname [enable|disable]
        set malformed [enable|disable]
        set max-cookie [enable|disable]
        set max-header-line [enable|disable]
        set max-url-param [enable|disable]
        set max-range-segment [enable|disable]
    next
end
end
set extended-log [enable|disable]
set external [disable|enable]
config method
    Description: Method restriction.
    set status [enable|disable]
    set log [enable|disable]
    set severity [high|medium|...]
    set default-allowed-methods {option1}, {option2}, ...
    config method-policy
        Description: HTTP method policy.
        edit <id>
            set pattern {string}
            set regex [enable|disable]
            set address {string}
            set allowed-methods {option1}, {option2}, ...
        next
    end
end
end
config signature
    Description: WAF signatures.
    config main-class
        Description: Main signature class.
        edit <id>
            set status [enable|disable]
            set action [allow|block|...]
            set log [enable|disable]
            set severity [high|medium|...]
        next
    end
    set disabled-sub-class <id1>, <id2>, ...
    set disabled-signature <id1>, <id2>, ...
    set credit-card-detection-threshold {integer}
    config custom-signature
        Description: Custom signature.
        edit <name>
            set status [enable|disable]
            set action [allow|block|...]
            set log [enable|disable]
            set severity [high|medium|...]
            set direction [request|response]
        end
    end
end

```



```

        set case-sensitivity [disable|enable]
        set pattern {string}
        set target {option1}, {option2}, ...
    next
end
end
config url-access
    Description: URL access list.
    edit <id>
        set address {string}
        set action [bypass|permit|...]
        set log [enable|disable]
        set severity [high|medium|...]
        config access-pattern
            Description: URL access pattern.
            edit <id>
                set srcaddr {string}
                set pattern {string}
                set regex [enable|disable]
                set negate [enable|disable]
            next
        end
    next
end
next
end
next
end

```

## config waf profile

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 1023	
extended-log	Enable/disable extended logging.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
external	Disable/Enable external HTTP Inspection.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable external inspection.		
	<i>enable</i>	Enable external inspection.		
name	WAF Profile name.	string	Maximum length: 35	

## config address-list

Parameter	Description	Type	Size	Default
status	Status.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
blocked-log	Enable/disable logging on blocked addresses.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
severity	Severity.	option	-	medium
	<b>Option</b>	<b>Description</b>		
	<i>high</i>	High severity.		
	<i>medium</i>	Medium severity.		
	<i>low</i>	Low severity.		
trusted-address <name>	Trusted address. Address name.	string	Maximum length: 79	
blocked-address <name>	Blocked address. Address name.	string	Maximum length: 79	

## config header-length

Parameter	Description	Type	Size	Default
status	Enable/disable the constraint.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

Parameter	Description	Type	Size	Default								
length	Length of HTTP header in bytes (0 to 2147483647).	integer	Minimum value: 0 Maximum value: 2147483647	8192								
action	Action.	option	-	allow								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow.</td></tr><tr><td><i>block</i></td><td>Block.</td></tr></table>				Option	Description	<i>allow</i>	Allow.	<i>block</i>	Block.		
	Option	Description										
	<i>allow</i>	Allow.										
<i>block</i>	Block.											
log	Enable/disable logging.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>				Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.		
	Option	Description										
	<i>enable</i>	Enable setting.										
<i>disable</i>	Disable setting.											
severity	Severity.	option	-	medium								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>high</i></td><td>High severity.</td></tr><tr><td><i>medium</i></td><td>Medium severity.</td></tr><tr><td><i>low</i></td><td>Low severity.</td></tr></table>				Option	Description	<i>high</i>	High severity.	<i>medium</i>	Medium severity.	<i>low</i>	Low severity.
	Option	Description										
	<i>high</i>	High severity.										
	<i>medium</i>	Medium severity.										
<i>low</i>	Low severity.											

### config content-length

Parameter	Description	Type	Size	Default						
status	Enable/disable the constraint.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>				Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.
	Option	Description								
	<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.									
length	Length of HTTP content in bytes (0 to 2147483647).	integer	Minimum value: 0 Maximum value: 2147483647	67108864						
action	Action.	option	-	allow						

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow.		
	<i>block</i>	Block.		
log	Enable/disable logging.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
severity	Severity.	option	-	medium
	<b>Option</b>	<b>Description</b>		
	<i>high</i>	High severity.		
	<i>medium</i>	Medium severity.		
	<i>low</i>	Low severity.		

#### config param-length

Parameter	Description	Type	Size	Default
status	Enable/disable the constraint.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
length	Maximum length of parameter in URL, HTTP POST request or HTTP body in bytes (0 to 2147483647).	integer	Minimum value: 0 Maximum value: 2147483647	8192
action	Action.	option	-	allow
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow.		
	<i>block</i>	Block.		
log	Enable/disable logging.	option	-	disable

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
severity	Severity.	option	-	medium
	<b>Option</b>	<b>Description</b>		
	<i>high</i>	High severity.		
	<i>medium</i>	Medium severity.		
	<i>low</i>	Low severity.		

### config line-length

Parameter	Description	Type	Size	Default
status	Enable/disable the constraint.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
length	Length of HTTP line in bytes (0 to 2147483647).	integer	Minimum value: 0 Maximum value: 2147483647	1024
action	Action.	option	-	allow
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow.		
	<i>block</i>	Block.		
log	Enable/disable logging.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
severity	Severity.	option	-	medium

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>high</i>	High severity.		
	<i>medium</i>	Medium severity.		
	<i>low</i>	Low severity.		

#### config url-param-length

Parameter	Description	Type	Size	Default
status	Enable/disable the constraint.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
length	Maximum length of URL parameter in bytes (0 to 2147483647).	integer	Minimum value: 0 Maximum value: 2147483647	8192
action	Action.	option	-	allow
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow.		
	<i>block</i>	Block.		
log	Enable/disable logging.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
severity	Severity.	option	-	medium
	<b>Option</b>	<b>Description</b>		
	<i>high</i>	High severity.		
	<i>medium</i>	Medium severity.		
	<i>low</i>	Low severity.		

## config version

Parameter	Description	Type	Size	Default
status	Enable/disable the constraint.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
action	Action.	option	-	allow
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow.		
	<i>block</i>	Block.		
log	Enable/disable logging.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
severity	Severity.	option	-	medium
	<b>Option</b>	<b>Description</b>		
	<i>high</i>	High severity.		
	<i>medium</i>	Medium severity.		
	<i>low</i>	Low severity.		

## config method

Parameter	Description	Type	Size	Default
status	Enable/disable the constraint.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
action	Action.	option	-	allow

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow.		
	<i>block</i>	Block.		
log	Enable/disable logging.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
severity	Severity.	option	-	medium
	<b>Option</b>	<b>Description</b>		
	<i>high</i>	High severity.		
	<i>medium</i>	Medium severity.		
	<i>low</i>	Low severity.		

### config method

Parameter	Description	Type	Size	Default
status	Status.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
log	Enable/disable logging.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
severity	Severity.	option	-	medium
	<b>Option</b>	<b>Description</b>		
	<i>high</i>	High severity		
	<i>medium</i>	medium severity		
	<i>low</i>	low severity		



Parameter	Description	Type	Size	Default
default-allowed-methods	Methods.	option	-	
	<b>Option</b>	<b>Description</b>		
	<i>get</i>	HTTP GET method.		
	<i>post</i>	HTTP POST method.		
	<i>put</i>	HTTP PUT method.		
	<i>head</i>	HTTP HEAD method.		
	<i>connect</i>	HTTP CONNECT method.		
	<i>trace</i>	HTTP TRACE method.		
	<i>options</i>	HTTP OPTIONS method.		
	<i>delete</i>	HTTP DELETE method.		
	<i>others</i>	Other HTTP methods.		

#### config hostname

Parameter	Description	Type	Size	Default						
status	Enable/disable the constraint.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
	Option	Description								
	<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.									
action	Action.	option	-	allow						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow.</td></tr><tr><td><i>block</i></td><td>Block.</td></tr></table>	Option	Description	<i>allow</i>	Allow.	<i>block</i>	Block.			
	Option	Description								
	<i>allow</i>	Allow.								
<i>block</i>	Block.									
log	Enable/disable logging.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
	Option	Description								
	<i>enable</i>	Enable setting.								
<i>disable</i>	Disable setting.									
severity	Severity.	option	-	medium						

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>high</i>	High severity.		
	<i>medium</i>	Medium severity.		
	<i>low</i>	Low severity.		

#### config malformed

Parameter	Description	Type	Size	Default
status	Enable/disable the constraint.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
action	Action.	option	-	allow
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow.		
	<i>block</i>	Block.		
log	Enable/disable logging.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
severity	Severity.	option	-	medium
	<b>Option</b>	<b>Description</b>		
	<i>high</i>	High severity.		
	<i>medium</i>	Medium severity.		
	<i>low</i>	Low severity.		

#### config max-cookie

Parameter	Description	Type	Size	Default
status	Enable/disable the constraint.	option	-	disable

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
max-cookie	Maximum number of cookies in HTTP request (0 to 2147483647).	integer	Minimum value: 0 Maximum value: 2147483647	16
action	Action.	option	-	allow
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow.		
	<i>block</i>	Block.		
log	Enable/disable logging.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
severity	Severity.	option	-	medium
	<b>Option</b>	<b>Description</b>		
	<i>high</i>	High severity.		
	<i>medium</i>	Medium severity.		
	<i>low</i>	Low severity.		

#### config max-header-line

Parameter	Description	Type	Size	Default
status	Enable/disable the constraint.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

Parameter	Description	Type	Size	Default
max-header-line	Maximum number HTTP header lines (0 to 2147483647).	integer	Minimum value: 0 Maximum value: 2147483647	32
action	Action.	option	-	allow
	<b>Option</b>		<b>Description</b>	
	<i>allow</i>	Allow.		
	<i>block</i>	Block.		
log	Enable/disable logging.	option	-	disable
	<b>Option</b>		<b>Description</b>	
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
severity	Severity.	option	-	medium
	<b>Option</b>		<b>Description</b>	
	<i>high</i>	High severity.		
	<i>medium</i>	Medium severity.		
	<i>low</i>	Low severity.		

#### config max-url-param

Parameter	Description	Type	Size	Default
status	Enable/disable the constraint.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
max-url-param	Maximum number of parameters in URL (0 to 2147483647).	integer	Minimum value: 0 Maximum value: 2147483647	16
action	Action.	option	-	allow

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow.		
	<i>block</i>	Block.		
log	Enable/disable logging.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
severity	Severity.	option	-	medium
	<b>Option</b>	<b>Description</b>		
	<i>high</i>	High severity.		
	<i>medium</i>	Medium severity.		
	<i>low</i>	Low severity.		

#### config max-range-segment

Parameter	Description	Type	Size	Default
status	Enable/disable the constraint.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
max-range-segment	Maximum number of range segments in HTTP range line (0 to 2147483647).	integer	Minimum value: 0 Maximum value: 2147483647	5
action	Action.	option	-	allow
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow.		
	<i>block</i>	Block.		
log	Enable/disable logging.	option	-	disable

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
severity	Severity.	option	-	medium
	<b>Option</b>	<b>Description</b>		
	<i>high</i>	High severity.		
	<i>medium</i>	Medium severity.		
	<i>low</i>	Low severity.		

### config exception

Parameter	Description	Type	Size	Default
id	Exception ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
pattern	URL pattern.	string	Maximum length: 511	
regex	Enable/disable regular expression based pattern match.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
address	Host address.	string	Maximum length: 79	
header-length	HTTP header length in request.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
content-length	HTTP content length in request.	option	-	disable

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
param-length	Maximum length of parameter in URL, HTTP POST request or HTTP body.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
line-length	HTTP line length in request.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
url-param-length	Maximum length of parameter in URL.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
version	Enable/disable HTTP version check.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
method	Enable/disable HTTP method check.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
hostname	Enable/disable hostname check.	option	-	disable

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
malformed	Enable/disable malformed HTTP request check.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
max-cookie	Maximum number of cookies in HTTP request.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
max-header-line	Maximum number of HTTP header line.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
max-url-param	Maximum number of parameters in URL.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
max-range-segment	Maximum number of range segments in HTTP range line.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		



### config method

Parameter	Description	Type	Size	Default
status	Enable/disable the constraint.	option	-	disable
action	Action.	option	-	allow
log	Enable/disable logging.	option	-	disable
severity	Severity.	option	-	medium

### config method

Parameter	Description	Type	Size	Default
status	Status.	option	-	disable
log	Enable/disable logging.	option	-	disable
severity	Severity.	option	-	medium
default-allowed-methods	Methods.	option	-	

### config method-policy

Parameter	Description	Type	Size	Default
id	HTTP method policy ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
pattern	URL pattern.	string	Maximum length: 511	
regex	Enable/disable regular expression based pattern match.	option	-	disable
	Option	Description		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
address	Host address.	string	Maximum length: 79	
allowed-methods	Allowed Methods.	option	-	

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>get</i>	HTTP GET method.		
	<i>post</i>	HTTP POST method.		
	<i>put</i>	HTTP PUT method.		
	<i>head</i>	HTTP HEAD method.		
	<i>connect</i>	HTTP CONNECT method.		
	<i>trace</i>	HTTP TRACE method.		
	<i>options</i>	HTTP OPTIONS method.		
	<i>delete</i>	HTTP DELETE method.		
	<i>others</i>	Other HTTP methods.		

### config signature

Parameter	Description	Type	Size	Default
disabled-sub-class <id>	Disabled signature subclasses. Signature subclass ID.	integer	Minimum value: 0 Maximum value: 4294967295	
disabled-signature <id>	Disabled signatures. Signature ID.	integer	Minimum value: 0 Maximum value: 4294967295	
credit-card-detection-threshold	The minimum number of Credit cards to detect violation.	integer	Minimum value: 0 Maximum value: 128	3

### config main-class

Parameter	Description	Type	Size	Default
id	Main signature class ID.	integer	Minimum value: 0 Maximum value: 4294967295	0

Parameter	Description	Type	Size	Default
status	Status.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
action	Action.	option	-	allow
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow.		
	<i>block</i>	Block.		
	<i>erase</i>	Erase credit card numbers.		
log	Enable/disable logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
severity	Severity.	option	-	medium
	<b>Option</b>	<b>Description</b>		
	<i>high</i>	High severity.		
	<i>medium</i>	Medium severity.		
	<i>low</i>	Low severity.		

#### config custom-signature

Parameter	Description	Type	Size	Default
name	Signature name.	string	Maximum length: 35	
status	Status.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
action	Action.	option	-	allow

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>allow</i>	Allow.		
	<i>block</i>	Block.		
	<i>erase</i>	Erase credit card numbers.		
log	Enable/disable logging.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
severity	Severity.	option	-	medium
	<b>Option</b>	<b>Description</b>		
	<i>high</i>	High severity.		
	<i>medium</i>	Medium severity.		
	<i>low</i>	Low severity.		
direction	Traffic direction.	option	-	request
	<b>Option</b>	<b>Description</b>		
	<i>request</i>	Match HTTP request.		
	<i>response</i>	Match HTTP response.		
case-sensitivity	Case sensitivity in pattern.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Case insensitive in pattern.		
	<i>enable</i>	Case sensitive in pattern.		
pattern	Match pattern.	string	Maximum length: 511	
target	Match HTTP target.	option	-	
	<b>Option</b>	<b>Description</b>		
	<i>arg</i>	HTTP arguments.		
	<i>arg-name</i>	Names of HTTP arguments.		
	<i>req-body</i>	HTTP request body.		

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>req-cookie</i>	HTTP request cookies.		
	<i>req-cookie-name</i>	HTTP request cookie names.		
	<i>req-filename</i>	HTTP request file name.		
	<i>req-header</i>	HTTP request headers.		
	<i>req-header-name</i>	HTTP request header names.		
	<i>req-raw-uri</i>	Raw URI of HTTP request.		
	<i>req-uri</i>	URI of HTTP request.		
	<i>resp-body</i>	HTTP response body.		
	<i>resp-hdr</i>	HTTP response headers.		
	<i>resp-status</i>	HTTP response status.		

### config url-access

Parameter	Description	Type	Size	Default
id	URL access ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
address	Host address.	string	Maximum length: 79	
action	Action.	option	-	permit
	<b>Option</b>	<b>Description</b>		
	<i>bypass</i>	Allow the HTTP request, also bypass further WAF scanning.		
	<i>permit</i>	Allow the HTTP request, and continue further WAF scanning.		
	<i>block</i>	Block HTTP request.		
log	Enable/disable logging.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

Parameter	Description	Type	Size	Default
severity	Severity.	option	-	medium
	<b>Option</b>	<b>Description</b>		
	<i>high</i>	High severity.		
	<i>medium</i>	Medium severity.		
	<i>low</i>	Low severity.		

### config access-pattern

Parameter	Description	Type	Size	Default
id	URL access pattern ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
srcaddr	Source address.	string	Maximum length: 79	
pattern	URL pattern.	string	Maximum length: 511	
regex	Enable/disable regular expression based pattern match.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
negate	Enable/disable match negation.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

### config waf signature

Hidden table for datasource.

```
config waf signature
    Description: Hidden table for datasource.
    edit <id>
        set desc {string}
```

```
next
end
```

## config waf signature

Parameter	Description	Type	Size	Default
desc	Signature description.	string	Maximum length: 511	
id	Signature ID.	integer	Minimum value: 0 Maximum value: 4294967295	0

## config waf sub-class

Hidden table for datasource.

```
config waf sub-class
  Description: Hidden table for datasource.
  edit <id>
    set name {string}
  next
end
```

## config waf sub-class

Parameter	Description	Type	Size	Default
id	Signature subclass ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
name	Signature subclass name.	string	Maximum length: 127	

## wanopt

This section includes syntax for the following commands:

- [config wanopt auth-group on page 1828](#)
- [config wanopt cache-service on page 1830](#)
- [config wanopt content-delivery-network-rule on page 1833](#)
- [config wanopt peer on page 1839](#)
- [config wanopt profile on page 1840](#)
- [config wanopt remote-storage on page 1849](#)
- [config wanopt settings on page 1850](#)
- [config wanopt webcache on page 1852](#)

### config wanopt auth-group



This command is available for model(s): FortiGate 1000D, FortiGate 101E, FortiGate 101F, FortiGate 1101E, FortiGate 1200D, FortiGate 1500DT, FortiGate 1500D, FortiGate 1801F, FortiGate 2000E, FortiGate 201E, FortiGate 201F, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3001F, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3301E, FortiGate 3401E, FortiGate 3501F, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 401E, FortiGate 401F, FortiGate 4201F, FortiGate 4401F, FortiGate 5001E1, FortiGate 501E, FortiGate 601E, FortiGate 601F, FortiGate 61E, FortiGate 61F, FortiGate 71F, FortiGate 800D, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 91E, FortiGate VM64, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 1100E, FortiGate 140E-POE, FortiGate 140E, FortiGate 1800F, FortiGate 200E, FortiGate 200F, FortiGate 2200E, FortiGate 3000F, FortiGate 300E, FortiGate 3300E, FortiGate 3400E, FortiGate 3500F, FortiGate 3600E, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4400F, FortiGate 5001E, FortiGate 500E, FortiGate 600E, FortiGate 600F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 70F, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 90E, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 80F 2R.

Configure WAN optimization authentication groups.

```
config wanopt auth-group
  Description: Configure WAN optimization authentication groups.
  edit <name>
    set auth-method [cert|psk]
    set cert {string}
```



```

        set peer {string}
        set peer-accept [any|defined|...]
        set psk {password}
    next
end

```

## config wanopt auth-group

Parameter	Description	Type	Size	Default								
auth-method	Select certificate or pre-shared key authentication for this authentication group.	option	-	cert								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>cert</i></td><td>Certificate authentication.</td></tr><tr><td><i>psk</i></td><td>Pre-shared secret key authentication.</td></tr></table>				Option	Description	<i>cert</i>	Certificate authentication.	<i>psk</i>	Pre-shared secret key authentication.		
Option	Description											
<i>cert</i>	Certificate authentication.											
<i>psk</i>	Pre-shared secret key authentication.											
cert	Name of certificate to identify this peer.	string	Maximum length: 35									
name	Auth-group name.	string	Maximum length: 35									
peer	If peer-accept is set to one, select the name of one peer to add to this authentication group. The peer must have added with the wanopt peer command.	string	Maximum length: 35									
peer-accept	Determine if this auth group accepts, any peer, a list of defined peers, or just one peer.	option	-	any								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>any</i></td><td>Accept any peer that can authenticate with this auth group.</td></tr><tr><td><i>defined</i></td><td>Accept only the peers added with the wanopt peer command.</td></tr><tr><td><i>one</i></td><td>Accept the peer added to this auth group using the peer option.</td></tr></table>				Option	Description	<i>any</i>	Accept any peer that can authenticate with this auth group.	<i>defined</i>	Accept only the peers added with the wanopt peer command.	<i>one</i>	Accept the peer added to this auth group using the peer option.
Option	Description											
<i>any</i>	Accept any peer that can authenticate with this auth group.											
<i>defined</i>	Accept only the peers added with the wanopt peer command.											
<i>one</i>	Accept the peer added to this auth group using the peer option.											
psk	Pre-shared key used by the peers in this authentication group.	password	Not Specified									

---

## config wanopt cache-service

---



This command is available for model(s): FortiGate 1000D, FortiGate 101E, FortiGate 101F, FortiGate 1101E, FortiGate 1200D, FortiGate 1500DT, FortiGate 1500D, FortiGate 1801F, FortiGate 2000E, FortiGate 201E, FortiGate 201F, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3001F, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3301E, FortiGate 3401E, FortiGate 3501F, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 401E, FortiGate 401F, FortiGate 4201F, FortiGate 4401F, FortiGate 5001E1, FortiGate 501E, FortiGate 601E, FortiGate 601F, FortiGate 61E, FortiGate 61F, FortiGate 71F, FortiGate 800D, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 91E, FortiGate VM64, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 1100E, FortiGate 140E-POE, FortiGate 140E, FortiGate 1800F, FortiGate 200E, FortiGate 200F, FortiGate 2200E, FortiGate 3000F, FortiGate 300E, FortiGate 3300E, FortiGate 3400E, FortiGate 3500F, FortiGate 3600E, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4400F, FortiGate 5001E, FortiGate 500E, FortiGate 600E, FortiGate 600F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 70F, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 90E, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 80F 2R.

---

Designate cache-service for wan-optimization and webcache.

```
config wanopt cache-service
  Description: Designate cache-service for wan-optimization and webcache.
  set acceptable-connections [any|peers]
  set collaboration [enable|disable]
  set device-id {string}
  config dst-peer
    Description: Modify cache-service destination peer list.
    edit <device-id>
      set auth-type {integer}
      set encode-type {integer}
      set priority {integer}
      set ip {ipv4-address-any}
    next
  end
  set prefer-scenario [balance|prefer-speed|...]
  config src-peer
    Description: Modify cache-service source peer list.
    edit <device-id>
      set auth-type {integer}
      set encode-type {integer}
      set priority {integer}
      set ip {ipv4-address-any}
    next
  end
end
```

## config wanopt cache-service

Parameter	Description	Type	Size	Default								
acceptable-connections	Set strategy when accepting cache collaboration connection.	option	-	any								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>any</i></td><td>We can accept any cache-collaboration connection.</td></tr><tr><td><i>peers</i></td><td>We can only accept connections that are already in src-peers.</td></tr></table>	Option	Description	<i>any</i>	We can accept any cache-collaboration connection.	<i>peers</i>	We can only accept connections that are already in src-peers.					
Option	Description											
<i>any</i>	We can accept any cache-collaboration connection.											
<i>peers</i>	We can only accept connections that are already in src-peers.											
collaboration	Enable/disable cache-collaboration between cache-service clusters.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable cache cache-collaboration.</td></tr><tr><td><i>disable</i></td><td>Disable cache cache-collaboration.</td></tr></table>	Option	Description	<i>enable</i>	Enable cache cache-collaboration.	<i>disable</i>	Disable cache cache-collaboration.					
Option	Description											
<i>enable</i>	Enable cache cache-collaboration.											
<i>disable</i>	Disable cache cache-collaboration.											
device-id	Set identifier for this cache device.	string	Maximum length: 35	default_dev_id								
prefer-scenario	Set the preferred cache behavior towards the balance between latency and hit-ratio.	option	-	balance								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>balance</i></td><td>Balance between speed and cache hit ratio.</td></tr><tr><td><i>prefer-speed</i></td><td>Prefer response speed at the expense of increased cache bypasses.</td></tr><tr><td><i>prefer-cache</i></td><td>Prefer improving hit-ratio through increasing latency tolerance.</td></tr></table>	Option	Description	<i>balance</i>	Balance between speed and cache hit ratio.	<i>prefer-speed</i>	Prefer response speed at the expense of increased cache bypasses.	<i>prefer-cache</i>	Prefer improving hit-ratio through increasing latency tolerance.			
Option	Description											
<i>balance</i>	Balance between speed and cache hit ratio.											
<i>prefer-speed</i>	Prefer response speed at the expense of increased cache bypasses.											
<i>prefer-cache</i>	Prefer improving hit-ratio through increasing latency tolerance.											

## config dst-peer

Parameter	Description	Type	Size	Default
device-id	Device ID of this peer.	string	Maximum length: 35	
auth-type	Set authentication type for this peer.	integer	Minimum value: 0 Maximum value: 255	0
encode-type	Set encode type for this peer.	integer	Minimum value: 0 Maximum value: 255	0

Parameter	Description	Type	Size	Default
priority	Set priority for this peer.	integer	Minimum value: 0 Maximum value: 255	1
ip	Set cluster IP address of this peer.	ipv4-address-any	Not Specified	0.0.0.0

### config src-peer

Parameter	Description	Type	Size	Default
device-id	Device ID of this peer.	string	Maximum length: 35	
auth-type	Set authentication type for this peer.	integer	Minimum value: 0 Maximum value: 255	0
encode-type	Set encode type for this peer.	integer	Minimum value: 0 Maximum value: 255	0
priority	Set priority for this peer.	integer	Minimum value: 0 Maximum value: 255	1
ip	Set cluster IP address of this peer.	ipv4-address-any	Not Specified	0.0.0.0

---

## config wanopt content-delivery-network-rule

---



This command is available for model(s): FortiGate 1000D, FortiGate 101E, FortiGate 101F, FortiGate 1101E, FortiGate 1200D, FortiGate 1500DT, FortiGate 1500D, FortiGate 1801F, FortiGate 2000E, FortiGate 201E, FortiGate 201F, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3001F, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3301E, FortiGate 3401E, FortiGate 3501F, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 401E, FortiGate 401F, FortiGate 4201F, FortiGate 4401F, FortiGate 5001E1, FortiGate 501E, FortiGate 601E, FortiGate 601F, FortiGate 61E, FortiGate 61F, FortiGate 71F, FortiGate 800D, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 91E, FortiGate VM64, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 1100E, FortiGate 140E-POE, FortiGate 140E, FortiGate 1800F, FortiGate 200E, FortiGate 200F, FortiGate 2200E, FortiGate 3000F, FortiGate 300E, FortiGate 3300E, FortiGate 3400E, FortiGate 3500F, FortiGate 3600E, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4400F, FortiGate 5001E, FortiGate 500E, FortiGate 600E, FortiGate 600F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 70F, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 90E, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 80F 2R.

---

### Configure WAN optimization content delivery network rules.

```
config wanopt content-delivery-network-rule
  Description: Configure WAN optimization content delivery network rules.
  edit <name>
    set category [vcache|youtube]
    set comment {var-string}
    set host-domain-name-suffix <name1>, <name2>, ...
    set request-cache-control [enable|disable]
    set response-cache-control [enable|disable]
    set response-expires [enable|disable]
    config rules
      Description: WAN optimization content delivery network rule entries.
      edit <name>
        set match-mode [all|any]
        set skip-rule-mode [all|any]
        config match-entries
          Description: List of entries to match.
          edit <id>
            set target [path|parameter|...]
            set pattern <string1>, <string2>, ...
          next
        end
      config skip-entries
        Description: List of entries to skip.
        edit <id>
          set target [path|parameter|...]
```

```

        set pattern <string1>, <string2>, ...
    next
end
config content-id
    Description: Content ID settings.
    set target [path|parameter|...]
    set start-str {string}
    set start-skip {integer}
    set start-direction [forward|backward]
    set end-str {string}
    set end-skip {integer}
    set end-direction [forward|backward]
    set range-str {string}
end
next
end
set status [enable|disable]
set updateserver [enable|disable]
next
end

```

## config wanopt content-delivery-network-rule

Parameter	Description	Type	Size	Default						
category	Content delivery network rule category.	option	-	vcache						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>vcache</td><td>Vcache content delivery network.</td></tr><tr><td>youtube</td><td>Youtube content delivery network.</td></tr></table>	Option	Description	vcache	Vcache content delivery network.	youtube	Youtube content delivery network.			
	Option	Description								
	vcache	Vcache content delivery network.								
youtube	Youtube content delivery network.									
comment	Comment about this CDN-rule.	var-string	Maximum length: 255							
host-domain-name-suffix <name>	Suffix portion of the fully qualified domain name. For example, fortinet.com in "www.fortinet.com". Suffix portion of the fully qualified domain name.	string	Maximum length: 79							
name	Name of table.	string	Maximum length: 35							
request-cache-control	Enable/disable HTTP request cache control.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>	Option	Description	enable	Enable setting.	disable	Disable setting.			
	Option	Description								
	enable	Enable setting.								
disable	Disable setting.									
response-cache-control	Enable/disable HTTP response cache control.	option	-	disable						

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
response-expires	Enable/disable HTTP response cache expires.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
status	Enable/disable WAN optimization content delivery network rules.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
updateserver	Enable/disable update server.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

## config rules

Parameter	Description	Type	Size	Default
name	WAN optimization content delivery network rule name.	string	Maximum length: 35	
match-mode	Match criteria for collecting content ID.	option	-	all
	<b>Option</b>	<b>Description</b>		
	<i>all</i>	Must match all of the match entries.		
	<i>any</i>	Must match any of the match entries.		
skip-rule-mode	Skip mode when evaluating skip-rules.	option	-	all

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>all</i>	Must match all skip entries.		
	<i>any</i>	Must match any skip entries.		

#### config match-entries

Parameter	Description	Type	Size	Default
id	Rule ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
target	Option in HTTP header or URL parameter to match.	option	-	path
	<b>Option</b>	<b>Description</b>		
	<i>path</i>	Match with the URL path.		
	<i>parameter</i>	Match with the URL parameters.		
	<i>referrer</i>	Match with the Referrer option in HTTP header.		
	<i>youtube-map</i>	Match Youtube content-id collection.		
	<i>youtube-id</i>	Match Youtube content-id.		
	<i>youku-id</i>	Match Youku content-id.		
pattern <string>	Pattern string for matching target (Referrer or URL pattern). For example, a, a*c, *a*, a*c*e, and *. Pattern strings.	string	Maximum length: 79	

#### config skip-entries

Parameter	Description	Type	Size	Default
id	Rule ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
target	Option in HTTP header or URL parameter to match.	option	-	path



Parameter	Description	Type	Size	Default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>path</i></td><td>Match with the URL path.</td></tr><tr><td><i>parameter</i></td><td>Match with the URL parameters.</td></tr><tr><td><i>referrer</i></td><td>Match with the Referrer option in HTTP header.</td></tr><tr><td><i>youtube-map</i></td><td>Match Youtube content-id collection.</td></tr><tr><td><i>youtube-id</i></td><td>Match Youtube content-id.</td></tr><tr><td><i>youku-id</i></td><td>Match Youku content-id.</td></tr></table>	Option	Description	<i>path</i>	Match with the URL path.	<i>parameter</i>	Match with the URL parameters.	<i>referrer</i>	Match with the Referrer option in HTTP header.	<i>youtube-map</i>	Match Youtube content-id collection.	<i>youtube-id</i>	Match Youtube content-id.	<i>youku-id</i>	Match Youku content-id.			
	Option	Description																
	<i>path</i>	Match with the URL path.																
	<i>parameter</i>	Match with the URL parameters.																
	<i>referrer</i>	Match with the Referrer option in HTTP header.																
	<i>youtube-map</i>	Match Youtube content-id collection.																
	<i>youtube-id</i>	Match Youtube content-id.																
<i>youku-id</i>	Match Youku content-id.																	
pattern <string>	Pattern string for matching target (Referrer or URL pattern). For example, a, a*c, *a*, a*c*e, and *. Pattern strings.	string	Maximum length: 79															

### config content-id

Parameter	Description	Type	Size	Default
target	Option in HTTP header or URL parameter to match.	option	-	path
	<b>Option</b>	<b>Description</b>		
	<i>path</i>	Match with the URL path.		
	<i>parameter</i>	Match with the URL parameters.		
	<i>referrer</i>	Match with the Referrer option in HTTP header.		
	<i>youtube-map</i>	Match Youtube content-id collection.		
	<i>youtube-id</i>	Match Youtube content-id.		
	<i>youku-id</i>	Match Youku content-id.		
	<i>hls-manifest</i>	Match with HLS manifest.		
	<i>dash-manifest</i>	Match with DASH manifest.		
	<i>hls-fragment</i>	Match HLS stream fragment.		
	<i>dash-fragment</i>	Match DASH stream fragment.		
start-str	String from which to start search.	string	Maximum length: 35	
start-skip	Number of characters in URL to skip after start-str has been matched.	integer	Minimum value: 0 Maximum value: 4294967295	0

Parameter	Description	Type	Size	Default						
start-direction	Search direction from start-str match.	option	-	forward						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>forward</i></td><td>Forward direction.</td></tr><tr><td><i>backward</i></td><td>Backward direction.</td></tr></table>				Option	Description	<i>forward</i>	Forward direction.	<i>backward</i>	Backward direction.
	Option	Description								
	<i>forward</i>	Forward direction.								
<i>backward</i>	Backward direction.									
end-str	String from which to end search.	string	Maximum length: 35							
end-skip	Number of characters in URL to skip after end-str has been matched.	integer	Minimum value: 0 Maximum value: 4294967295	0						
end-direction	Search direction from end-str match.	option	-	forward						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>forward</i></td><td>Forward direction.</td></tr><tr><td><i>backward</i></td><td>Backward direction.</td></tr></table>				Option	Description	<i>forward</i>	Forward direction.	<i>backward</i>	Backward direction.
	Option	Description								
	<i>forward</i>	Forward direction.								
<i>backward</i>	Backward direction.									
range-str	Name of content ID within the start string and end string.	string	Maximum length: 35							

## config wanopt peer



This command is available for model(s): FortiGate 1000D, FortiGate 101E, FortiGate 101F, FortiGate 1101E, FortiGate 1200D, FortiGate 1500DT, FortiGate 1500D, FortiGate 1801F, FortiGate 2000E, FortiGate 201E, FortiGate 201F, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3001F, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3301E, FortiGate 3401E, FortiGate 3501F, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 401E, FortiGate 401F, FortiGate 4201F, FortiGate 4401F, FortiGate 5001E1, FortiGate 501E, FortiGate 601E, FortiGate 601F, FortiGate 61E, FortiGate 61F, FortiGate 71F, FortiGate 800D, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 91E, FortiGate VM64, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 1100E, FortiGate 140E-POE, FortiGate 140E, FortiGate 1800F, FortiGate 200E, FortiGate 200F, FortiGate 2200E, FortiGate 3000F, FortiGate 300E, FortiGate 3300E, FortiGate 3400E, FortiGate 3500F, FortiGate 3600E, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4400F, FortiGate 5001E, FortiGate 500E, FortiGate 600E, FortiGate 600F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 70F, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 90E, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 80F 2R.

Configure WAN optimization peers.

```
config wanopt peer
    Description: Configure WAN optimization peers.
    edit <peer-host-id>
        set ip {ipv4-address-any}
    next
end
```

## config wanopt peer

Parameter	Description	Type	Size	Default
ip	Peer IP address.	ipv4-address-any	Not Specified	0.0.0.0
peer-host-id	Peer host ID.	string	Maximum length: 35	

## config wanopt profile



This command is available for model(s): FortiGate 1000D, FortiGate 101E, FortiGate 101F, FortiGate 1101E, FortiGate 1200D, FortiGate 1500DT, FortiGate 1500D, FortiGate 1801F, FortiGate 2000E, FortiGate 201E, FortiGate 201F, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3001F, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3301E, FortiGate 3401E, FortiGate 3501F, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 401E, FortiGate 401F, FortiGate 4201F, FortiGate 4401F, FortiGate 5001E1, FortiGate 501E, FortiGate 601E, FortiGate 601F, FortiGate 61E, FortiGate 61F, FortiGate 71F, FortiGate 800D, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 91E, FortiGate VM64, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 1100E, FortiGate 140E-POE, FortiGate 140E, FortiGate 1800F, FortiGate 200E, FortiGate 200F, FortiGate 2200E, FortiGate 3000F, FortiGate 300E, FortiGate 3300E, FortiGate 3400E, FortiGate 3500F, FortiGate 3600E, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4400F, FortiGate 5001E, FortiGate 500E, FortiGate 600E, FortiGate 600F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 70F, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 90E, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 80F 2R.

Configure WAN optimization profiles.

```
config wanopt profile
  Description: Configure WAN optimization profiles.
  edit <name>
    set auth-group {string}
    config cifs
      Description: Enable/disable CIFS (Windows sharing) WAN Optimization and
configure CIFS WAN Optimization features.
      set status [enable|disable]
      set secure-tunnel [enable|disable]
      set byte-caching [enable|disable]
      set prefer-chunking [dynamic|fix]
      set protocol-opt [protocol|tcp]
      set tunnel-sharing [shared|express-shared|...]
      set log-traffic [enable|disable]
    end
    set comments {var-string}
    config ftp
      Description: Enable/disable FTP WAN Optimization and configure FTP WAN
Optimization features.
      set status [enable|disable]
      set secure-tunnel [enable|disable]
      set byte-caching [enable|disable]
      set ssl [enable|disable]
      set prefer-chunking [dynamic|fix]
      set protocol-opt [protocol|tcp]
```

```

        set tunnel-sharing [shared|express-shared|...]
        set log-traffic [enable|disable]
    end
    config http
        Description: Enable/disable HTTP WAN Optimization and configure HTTP WAN
        Optimization features.
        set status [enable|disable]
        set secure-tunnel [enable|disable]
        set byte-caching [enable|disable]
        set ssl [enable|disable]
        set prefer-chunking [dynamic|fix]
        set protocol-opt [protocol|tcp]
        set tunnel-sharing [shared|express-shared|...]
        set log-traffic [enable|disable]
    end
    config mapi
        Description: Enable/disable MAPI email WAN Optimization and configure MAPI WAN
        Optimization features.
        set status [enable|disable]
        set secure-tunnel [enable|disable]
        set byte-caching [enable|disable]
        set tunnel-sharing [shared|express-shared|...]
        set log-traffic [enable|disable]
    end
    config tcp
        Description: Enable/disable TCP WAN Optimization and configure TCP WAN
        Optimization features.
        set status [enable|disable]
        set secure-tunnel [enable|disable]
        set byte-caching [enable|disable]
        set byte-caching-opt [mem-only|mem-disk]
        set tunnel-sharing [shared|express-shared|...]
        set log-traffic [enable|disable]
        set port {user}
        set ssl [enable|disable]
        set ssl-port {user}
    end
    set transparent [enable|disable]
next
end

```

## config wanopt profile

Parameter	Description	Type	Size	Default
auth-group	Optionally add an authentication group to restrict access to the WAN Optimization tunnel to peers in the authentication group.	string	Maximum length: 35	
comments	Comment.	var-string	Maximum length: 255	
name	Profile name.	string	Maximum length: 35	

Parameter	Description	Type	Size	Default
transparent	Enable/disable transparent mode.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Determine if WAN Optimization changes client packet source addresses. Affects the routing configuration on the server network.		
	<i>disable</i>	Disable transparent mode. Client packets source addresses are changed to the source address of the FortiGate internal interface. Similar to source NAT.		

## config cifs

Parameter	Description	Type	Size	Default
status	Enable/disable WAN Optimization.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable WAN Optimization.		
	<i>disable</i>	Disable WAN Optimization.		
secure-tunnel	Enable/disable securing the WAN Opt tunnel using SSL. Secure and non-secure tunnels use the same TCP port (7810).	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable SSL-secured tunnelling.		
	<i>disable</i>	Disable SSL-secured tunnelling.		
byte-caching	Enable/disable byte-caching. Byte caching reduces the amount of traffic by caching file data sent across the WAN and in future serving if from the cache.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable byte-caching.		
	<i>disable</i>	Disable byte-caching.		
prefer-chunking	Select dynamic or fixed-size data chunking for WAN Optimization.	option	-	fix
	<b>Option</b>	<b>Description</b>		
	<i>dynamic</i>	Select dynamic data chunking to help to detect persistent data chunks in a changed file or in an embedded unknown protocol.		
	<i>fix</i>	Select fixed data chunking.		

Parameter	Description	Type	Size	Default								
protocol-opt	Select protocol specific optimization or generic TCP optimization.	option	-	protocol								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>protocol</i></td><td>Using protocol-specific optimization.</td></tr><tr><td><i>tcp</i></td><td>Using generic TCP optimization.</td></tr></table>	Option	Description	<i>protocol</i>	Using protocol-specific optimization.	<i>tcp</i>	Using generic TCP optimization.					
Option	Description											
<i>protocol</i>	Using protocol-specific optimization.											
<i>tcp</i>	Using generic TCP optimization.											
tunnel-sharing	Tunnel sharing mode for aggressive/non-aggressive and/or interactive/non-interactive protocols.	option	-	private								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>shared</i></td><td>For profiles that accept nonaggressive and non-interactive protocols.</td></tr><tr><td><i>express-shared</i></td><td>For profiles that accept interactive protocols such as Telnet.</td></tr><tr><td><i>private</i></td><td>For profiles that accept aggressive protocols such as HTTP and FTP so that these aggressive protocols do not share tunnels with less-aggressive protocols.</td></tr></table>	Option	Description	<i>shared</i>	For profiles that accept nonaggressive and non-interactive protocols.	<i>express-shared</i>	For profiles that accept interactive protocols such as Telnet.	<i>private</i>	For profiles that accept aggressive protocols such as HTTP and FTP so that these aggressive protocols do not share tunnels with less-aggressive protocols.			
Option	Description											
<i>shared</i>	For profiles that accept nonaggressive and non-interactive protocols.											
<i>express-shared</i>	For profiles that accept interactive protocols such as Telnet.											
<i>private</i>	For profiles that accept aggressive protocols such as HTTP and FTP so that these aggressive protocols do not share tunnels with less-aggressive protocols.											
log-traffic	Enable/disable logging.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable logging.</td></tr><tr><td><i>disable</i></td><td>Disable logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable logging.	<i>disable</i>	Disable logging.					
Option	Description											
<i>enable</i>	Enable logging.											
<i>disable</i>	Disable logging.											

## config ftp

Parameter	Description	Type	Size	Default						
status	Enable/disable WAN Optimization.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable WAN Optimization.</td></tr><tr><td><i>disable</i></td><td>Disable WAN Optimization.</td></tr></table>				Option	Description	<i>enable</i>	Enable WAN Optimization.	<i>disable</i>	Disable WAN Optimization.
	Option	Description								
	<i>enable</i>	Enable WAN Optimization.								
	<i>disable</i>	Disable WAN Optimization.								
secure-tunnel	Enable/disable securing the WAN Opt tunnel using SSL. Secure and non-secure tunnels use the same TCP port (7810).	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable SSL-secured tunnelling.</td></tr><tr><td><i>disable</i></td><td>Disable SSL-secured tunnelling.</td></tr></table>				Option	Description	<i>enable</i>	Enable SSL-secured tunnelling.	<i>disable</i>	Disable SSL-secured tunnelling.
	Option	Description								
	<i>enable</i>	Enable SSL-secured tunnelling.								
	<i>disable</i>	Disable SSL-secured tunnelling.								

Parameter	Description	Type	Size	Default								
byte-caching	Enable/disable byte-caching. Byte caching reduces the amount of traffic by caching file data sent across the WAN and in future serving if from the cache.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable byte-caching.</td></tr><tr><td><i>disable</i></td><td>Disable byte-caching.</td></tr></table>	Option	Description	<i>enable</i>	Enable byte-caching.	<i>disable</i>	Disable byte-caching.					
Option	Description											
<i>enable</i>	Enable byte-caching.											
<i>disable</i>	Disable byte-caching.											
ssl	Enable/disable SSL/TLS offloading (hardware acceleration) for traffic in this tunnel.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable SSL/TLS offloading.</td></tr><tr><td><i>disable</i></td><td>Disable SSL/TLS offloading.</td></tr></table>	Option	Description	<i>enable</i>	Enable SSL/TLS offloading.	<i>disable</i>	Disable SSL/TLS offloading.					
Option	Description											
<i>enable</i>	Enable SSL/TLS offloading.											
<i>disable</i>	Disable SSL/TLS offloading.											
prefer-chunking	Select dynamic or fixed-size data chunking for WAN Optimization.	option	-	fix								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>dynamic</i></td><td>Select dynamic data chunking to help to detect persistent data chunks in a changed file or in an embedded unknown protocol.</td></tr><tr><td><i>fix</i></td><td>Select fixed data chunking.</td></tr></table>	Option	Description	<i>dynamic</i>	Select dynamic data chunking to help to detect persistent data chunks in a changed file or in an embedded unknown protocol.	<i>fix</i>	Select fixed data chunking.					
Option	Description											
<i>dynamic</i>	Select dynamic data chunking to help to detect persistent data chunks in a changed file or in an embedded unknown protocol.											
<i>fix</i>	Select fixed data chunking.											
protocol-opt	Select protocol specific optimization or generic TCP optimization.	option	-	protocol								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>protocol</i></td><td>Using protocol-specific optimization.</td></tr><tr><td><i>tcp</i></td><td>Using generic TCP optimization.</td></tr></table>	Option	Description	<i>protocol</i>	Using protocol-specific optimization.	<i>tcp</i>	Using generic TCP optimization.					
Option	Description											
<i>protocol</i>	Using protocol-specific optimization.											
<i>tcp</i>	Using generic TCP optimization.											
tunnel-sharing	Tunnel sharing mode for aggressive/non-aggressive and/or interactive/non-interactive protocols.	option	-	private								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>shared</i></td><td>For profiles that accept nonaggressive and non-interactive protocols.</td></tr><tr><td><i>express-shared</i></td><td>For profiles that accept interactive protocols such as Telnet.</td></tr><tr><td><i>private</i></td><td>For profiles that accept aggressive protocols such as HTTP and FTP so that these aggressive protocols do not share tunnels with less-aggressive protocols.</td></tr></table>	Option	Description	<i>shared</i>	For profiles that accept nonaggressive and non-interactive protocols.	<i>express-shared</i>	For profiles that accept interactive protocols such as Telnet.	<i>private</i>	For profiles that accept aggressive protocols such as HTTP and FTP so that these aggressive protocols do not share tunnels with less-aggressive protocols.			
Option	Description											
<i>shared</i>	For profiles that accept nonaggressive and non-interactive protocols.											
<i>express-shared</i>	For profiles that accept interactive protocols such as Telnet.											
<i>private</i>	For profiles that accept aggressive protocols such as HTTP and FTP so that these aggressive protocols do not share tunnels with less-aggressive protocols.											
log-traffic	Enable/disable logging.	option	-	enable								



Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable logging.		
	<i>disable</i>	Disable logging.		

## config http

Parameter	Description	Type	Size	Default
status	Enable/disable WAN Optimization.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable WAN Optimization.		
	<i>disable</i>	Disable WAN Optimization.		
secure-tunnel	Enable/disable securing the WAN Opt tunnel using SSL. Secure and non-secure tunnels use the same TCP port (7810).	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable SSL-secured tunnelling.		
	<i>disable</i>	Disable SSL-secured tunnelling.		
byte-caching	Enable/disable byte-caching. Byte caching reduces the amount of traffic by caching file data sent across the WAN and in future serving if from the cache.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable byte-caching.		
	<i>disable</i>	Disable byte-caching.		
ssl	Enable/disable SSL/TLS offloading (hardware acceleration) for traffic in this tunnel.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable SSL/TLS offloading.		
	<i>disable</i>	Disable SSL/TLS offloading.		
prefer-chunking	Select dynamic or fixed-size data chunking for WAN Optimization.	option	-	fix

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>dynamic</i>	Select dynamic data chunking to help to detect persistent data chunks in a changed file or in an embedded unknown protocol.		
	<i>fix</i>	Select fixed data chunking.		
protocol-opt	Select protocol specific optimization or generic TCP optimization.	option	-	protocol
	<b>Option</b>	<b>Description</b>		
	<i>protocol</i>	Using protocol-specific optimization.		
	<i>tcp</i>	Using generic TCP optimization.		
tunnel-sharing	Tunnel sharing mode for aggressive/non-aggressive and/or interactive/non-interactive protocols.	option	-	private
	<b>Option</b>	<b>Description</b>		
	<i>shared</i>	For profiles that accept nonaggressive and non-interactive protocols.		
	<i>express-shared</i>	For profiles that accept interactive protocols such as Telnet.		
	<i>private</i>	For profiles that accept aggressive protocols such as HTTP and FTP so that these aggressive protocols do not share tunnels with less-aggressive protocols.		
log-traffic	Enable/disable logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable logging.		
	<i>disable</i>	Disable logging.		

## config mapi

Parameter	Description	Type	Size	Default						
status	Enable/disable WAN Optimization.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable WAN Optimization.</td></tr><tr><td><i>disable</i></td><td>Disable WAN Optimization.</td></tr></table>				Option	Description	<i>enable</i>	Enable WAN Optimization.	<i>disable</i>	Disable WAN Optimization.
	Option	Description								
	<i>enable</i>	Enable WAN Optimization.								
<i>disable</i>	Disable WAN Optimization.									
secure-tunnel	Enable/disable securing the WAN Opt tunnel using SSL. Secure and non-secure tunnels use the same TCP port (7810).	option	-	disable						

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable SSL-secured tunnelling.		
	<i>disable</i>	Disable SSL-secured tunnelling.		
byte-caching	Enable/disable byte-caching. Byte caching reduces the amount of traffic by caching file data sent across the WAN and in future serving if from the cache.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable byte-caching.		
	<i>disable</i>	Disable byte-caching.		
tunnel-sharing	Tunnel sharing mode for aggressive/non-aggressive and/or interactive/non-interactive protocols.	option	-	private
	<b>Option</b>	<b>Description</b>		
	<i>shared</i>	For profiles that accept nonaggressive and non-interactive protocols.		
	<i>express-shared</i>	For profiles that accept interactive protocols such as Telnet.		
	<i>private</i>	For profiles that accept aggressive protocols such as HTTP and FTP so that these aggressive protocols do not share tunnels with less-aggressive protocols.		
log-traffic	Enable/disable logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable logging.		
	<i>disable</i>	Disable logging.		

## config tcp

Parameter	Description	Type	Size	Default
status	Enable/disable WAN Optimization.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable WAN Optimization.		
	<i>disable</i>	Disable WAN Optimization.		
secure-tunnel	Enable/disable securing the WAN Opt tunnel using SSL. Secure and non-secure tunnels use the same TCP port (7810).	option	-	disable

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable SSL-secured tunnelling.		
	<i>disable</i>	Disable SSL-secured tunnelling.		
byte-caching	Enable/disable byte-caching. Byte caching reduces the amount of traffic by caching file data sent across the WAN and in future serving it from the cache.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable byte-caching.		
	<i>disable</i>	Disable byte-caching.		
byte-caching-opt	Select whether TCP byte-caching uses system memory only or both memory and disk space.	option	-	mem-only
	<b>Option</b>	<b>Description</b>		
	<i>mem-only</i>	Byte caching with memory only.		
	<i>mem-disk</i>	Byte caching with memory and disk.		
tunnel-sharing	Tunnel sharing mode for aggressive/non-aggressive and/or interactive/non-interactive protocols.	option	-	private
	<b>Option</b>	<b>Description</b>		
	<i>shared</i>	For profiles that accept nonaggressive and non-interactive protocols.		
	<i>express-shared</i>	For profiles that accept interactive protocols such as Telnet.		
	<i>private</i>	For profiles that accept aggressive protocols such as HTTP and FTP so that these aggressive protocols do not share tunnels with less-aggressive protocols.		
log-traffic	Enable/disable logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable logging.		
	<i>disable</i>	Disable logging.		
port	Port numbers or port number ranges for TCP. Only packets with a destination port number that matches this port number or range are accepted by this profile.	user	Not Specified	
ssl	Enable/disable SSL/TLS offloading (hardware acceleration) for traffic in this tunnel.	option	-	disable

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable SSL/TLS offloading.		
	<i>disable</i>	Disable SSL/TLS offloading.		
ssl-port	Port numbers or port number ranges on which to expect HTTPS traffic for SSL/TLS offloading.	user	Not Specified	

## config wanopt remote-storage



This command is available for model(s): FortiGate 1000D, FortiGate 101E, FortiGate 101F, FortiGate 1101E, FortiGate 1200D, FortiGate 1500DT, FortiGate 1500D, FortiGate 1801F, FortiGate 2000E, FortiGate 201E, FortiGate 201F, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3001F, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3301E, FortiGate 3401E, FortiGate 3501F, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 401E, FortiGate 401F, FortiGate 4201F, FortiGate 4401F, FortiGate 5001E1, FortiGate 501E, FortiGate 601E, FortiGate 601F, FortiGate 61E, FortiGate 61F, FortiGate 71F, FortiGate 800D, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 91E, FortiGate VM64, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 1100E, FortiGate 140E-POE, FortiGate 140E, FortiGate 1800F, FortiGate 200E, FortiGate 200F, FortiGate 2200E, FortiGate 3000F, FortiGate 300E, FortiGate 3300E, FortiGate 3400E, FortiGate 3500F, FortiGate 3600E, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4400F, FortiGate 5001E, FortiGate 500E, FortiGate 600E, FortiGate 600F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 70F, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 90E, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 80F 2R.

Configure a remote cache device as Web cache storage.

```
config wanopt remote-storage
    Description: Configure a remote cache device as Web cache storage.
    set local-cache-id {string}
    set remote-cache-id {string}
    set remote-cache-ip {ipv4-address-any}
    set status [disable|enable]
end
```

## config wanopt remote-storage

Parameter	Description	Type	Size	Default
local-cache-id	ID that this device uses to connect to the remote device.	string	Maximum length: 35	
remote-cache-id	ID of the remote device to which the device connects.	string	Maximum length: 35	
remote-cache-ip	IP address of the remote device to which the device connects.	ipv4-address-any	Not Specified	0.0.0.0
status	Enable/disable using remote device as Web cache storage.	option	-	disable
		Option	Description	
		disable	Use local disks as Web cache storage.	
		enable	Use a remote device as Web cache storage.	

## config wanopt settings



This command is available for model(s): FortiGate 1000D, FortiGate 101E, FortiGate 101F, FortiGate 1101E, FortiGate 1200D, FortiGate 1500DT, FortiGate 1500D, FortiGate 1801F, FortiGate 2000E, FortiGate 201E, FortiGate 201F, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3001F, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3301E, FortiGate 3401E, FortiGate 3501F, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 401E, FortiGate 401F, FortiGate 4201F, FortiGate 4401F, FortiGate 5001E1, FortiGate 501E, FortiGate 601E, FortiGate 601F, FortiGate 61E, FortiGate 61F, FortiGate 71F, FortiGate 800D, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 91E, FortiGate VM64, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 1100E, FortiGate 140E-POE, FortiGate 140E, FortiGate 1800F, FortiGate 200E, FortiGate 200F, FortiGate 2200E, FortiGate 3000F, FortiGate 300E, FortiGate 3300E, FortiGate 3400E, FortiGate 3500F, FortiGate 3600E, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4400F, FortiGate 5001E, FortiGate 500E, FortiGate 600E, FortiGate 600F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 70F, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 90E, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 80F 2R.

Configure WAN optimization settings.

```

config wanopt settings
    Description: Configure WAN optimization settings.
    set auto-detect-algorithm [simple|diff-req-resp]
    set host-id {string}
    set tunnel-optimization [memory-usage|balanced|...]
    set tunnel-ssl-algorithm [high|medium|...]
end

```

## config wanopt settings

Parameter	Description	Type	Size	Default								
auto-detect-algorithm	Auto detection algorithms used in tunnel negotiations.	option	-	simple								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>simple</i></td><td>Use the same TCP option value in SYN/SYNACK packets. Backward compatible.</td></tr><tr><td><i>diff-req-resp</i></td><td>Use different TCP option values in SYN/SYNACK packets to avoid false positive detection.</td></tr></table>				Option	Description	<i>simple</i>	Use the same TCP option value in SYN/SYNACK packets. Backward compatible.	<i>diff-req-resp</i>	Use different TCP option values in SYN/SYNACK packets to avoid false positive detection.		
Option	Description											
<i>simple</i>	Use the same TCP option value in SYN/SYNACK packets. Backward compatible.											
<i>diff-req-resp</i>	Use different TCP option values in SYN/SYNACK packets to avoid false positive detection.											
host-id	Local host ID (must also be entered in the remote FortiGate's peer list).	string	Maximum length: 35	default-id								
tunnel-optimization	WANOpt tunnel optimization option.	option	-	balanced **								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>memory-usage</i></td><td>Optimize tunnel for low system memory usage.</td></tr><tr><td><i>balanced</i></td><td>Optimize tunnel to balance between system memory usage and throughput.</td></tr><tr><td><i>throughput</i></td><td>Optimize tunnel for throughput.</td></tr></table>				Option	Description	<i>memory-usage</i>	Optimize tunnel for low system memory usage.	<i>balanced</i>	Optimize tunnel to balance between system memory usage and throughput.	<i>throughput</i>	Optimize tunnel for throughput.
Option	Description											
<i>memory-usage</i>	Optimize tunnel for low system memory usage.											
<i>balanced</i>	Optimize tunnel to balance between system memory usage and throughput.											
<i>throughput</i>	Optimize tunnel for throughput.											
tunnel-ssl-algorithm	Relative strength of encryption algorithms accepted during tunnel negotiation.	option	-	high								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>high</i></td><td>High encryption. Allow only AES and ChaCha.</td></tr><tr><td><i>medium</i></td><td>Medium encryption. Allow AES, ChaCha, 3DES, and RC4.</td></tr><tr><td><i>low</i></td><td>Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.</td></tr></table>				Option	Description	<i>high</i>	High encryption. Allow only AES and ChaCha.	<i>medium</i>	Medium encryption. Allow AES, ChaCha, 3DES, and RC4.	<i>low</i>	Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.
Option	Description											
<i>high</i>	High encryption. Allow only AES and ChaCha.											
<i>medium</i>	Medium encryption. Allow AES, ChaCha, 3DES, and RC4.											
<i>low</i>	Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.											

\*\* Values may differ between models.

---

## config wanopt webcache

---



This command is available for model(s): FortiGate 1000D, FortiGate 101E, FortiGate 101F, FortiGate 1101E, FortiGate 1200D, FortiGate 1500DT, FortiGate 1500D, FortiGate 1801F, FortiGate 2000E, FortiGate 201E, FortiGate 201F, FortiGate 2201E, FortiGate 2500E, FortiGate 2600F, FortiGate 2601F, FortiGate 3000D, FortiGate 3001F, FortiGate 301E, FortiGate 3100D, FortiGate 3200D, FortiGate 3301E, FortiGate 3401E, FortiGate 3501F, FortiGate 3601E, FortiGate 3700D, FortiGate 3800D, FortiGate 401E, FortiGate 401F, FortiGate 4201F, FortiGate 4401F, FortiGate 5001E1, FortiGate 501E, FortiGate 601E, FortiGate 601F, FortiGate 61E, FortiGate 61F, FortiGate 71F, FortiGate 800D, FortiGate 81E-POE, FortiGate 81E, FortiGate 81F-POE, FortiGate 81F, FortiGate 900D, FortiGate 91E, FortiGate VM64, FortiWiFi 61E, FortiWiFi 61F, FortiWiFi 81F 2R 3G4G-POE, FortiWiFi 81F 2R-POE, FortiWiFi 81F 2R.

It is not available for: FortiGate 100EF, FortiGate 100E, FortiGate 100F, FortiGate 1100E, FortiGate 140E-POE, FortiGate 140E, FortiGate 1800F, FortiGate 200E, FortiGate 200F, FortiGate 2200E, FortiGate 3000F, FortiGate 300E, FortiGate 3300E, FortiGate 3400E, FortiGate 3500F, FortiGate 3600E, FortiGate 3960E, FortiGate 3980E, FortiGate 400E Bypass, FortiGate 400E, FortiGate 400F, FortiGate 40F 3G4G, FortiGate 40F, FortiGate 4200F, FortiGate 4400F, FortiGate 5001E, FortiGate 500E, FortiGate 600E, FortiGate 600F, FortiGate 60E DSLJ, FortiGate 60E DSL, FortiGate 60E-POE, FortiGate 60E, FortiGate 60F, FortiGate 70F, FortiGate 80E-POE, FortiGate 80E, FortiGate 80F Bypass, FortiGate 80F-POE, FortiGate 80F, FortiGate 90E, FortiGateRugged 60F 3G4G, FortiGateRugged 60F, FortiWiFi 40F 3G4G, FortiWiFi 40F, FortiWiFi 60E DSLJ, FortiWiFi 60E DSL, FortiWiFi 60E, FortiWiFi 60F, FortiWiFi 80F 2R.

---

Configure global Web cache settings.

```
config wanopt webcache
    Description: Configure global Web cache settings.
    set always-revalidate [enable|disable]
    set cache-by-default [enable|disable]
    set cache-cookie [enable|disable]
    set cache-expired [enable|disable]
    set default-ttl {integer}
    set external [enable|disable]
    set fresh-factor {integer}
    set host-validate [enable|disable]
    set ignore-conditional [enable|disable]
    set ignore-ie-reload [enable|disable]
    set ignore-ims [enable|disable]
    set ignore-pnc [enable|disable]
    set max-object-size {integer}
    set max-ttl {integer}
    set min-ttl {integer}
    set neg-resp-time {integer}
    set reval-pnc [enable|disable]
end
```



## config wanopt webcache

Parameter	Description	Type	Size	Default						
always-revalidate	Enable/disable revalidation of requested cached objects, which have content on the server, before serving it to the client.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable revalidation of requested cached objects.</td></tr><tr><td><i>disable</i></td><td>Disable revalidation of requested cached objects.</td></tr></table>	Option	Description	<i>enable</i>	Enable revalidation of requested cached objects.	<i>disable</i>	Disable revalidation of requested cached objects.			
Option	Description									
<i>enable</i>	Enable revalidation of requested cached objects.									
<i>disable</i>	Disable revalidation of requested cached objects.									
cache-by-default	Enable/disable caching content that lacks explicit caching policies from the server.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable caching content that lacks explicit caching policies.</td></tr><tr><td><i>disable</i></td><td>Disable caching content that lacks explicit caching policies.</td></tr></table>	Option	Description	<i>enable</i>	Enable caching content that lacks explicit caching policies.	<i>disable</i>	Disable caching content that lacks explicit caching policies.			
Option	Description									
<i>enable</i>	Enable caching content that lacks explicit caching policies.									
<i>disable</i>	Disable caching content that lacks explicit caching policies.									
cache-cookie	Enable/disable caching cookies. Since cookies contain information for or about individual users, they not usually cached.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Cache cookies.</td></tr><tr><td><i>disable</i></td><td>Do not cache cookies.</td></tr></table>	Option	Description	<i>enable</i>	Cache cookies.	<i>disable</i>	Do not cache cookies.			
Option	Description									
<i>enable</i>	Cache cookies.									
<i>disable</i>	Do not cache cookies.									
cache-expired	Enable/disable caching type-1 objects that are already expired on arrival.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
default-ttl	Default object expiry time. This only applies to those objects that do not have an expiry time set by the web server.	integer	Minimum value: 1 Maximum value: 5256000	1440						
external	Enable/disable external Web caching.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable external Web caching.</td></tr><tr><td><i>disable</i></td><td>Disable external Web caching.</td></tr></table>	Option	Description	<i>enable</i>	Enable external Web caching.	<i>disable</i>	Disable external Web caching.			
Option	Description									
<i>enable</i>	Enable external Web caching.									
<i>disable</i>	Disable external Web caching.									

Parameter	Description	Type	Size	Default						
fresh-factor	Frequency that the server is checked to see if any objects have expired. The higher the fresh factor, the less often the checks occur.	integer	Minimum value: 1 Maximum value: 100	100						
host-validate	Enable/disable validating "Host:" with original server IP.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable validating "Host:" with original server IP.</td></tr><tr><td><i>disable</i></td><td>Disable validating "Host:" with original server IP.</td></tr></table>	Option	Description	<i>enable</i>	Enable validating "Host:" with original server IP.	<i>disable</i>	Disable validating "Host:" with original server IP.			
Option	Description									
<i>enable</i>	Enable validating "Host:" with original server IP.									
<i>disable</i>	Disable validating "Host:" with original server IP.									
ignore-conditional	Enable/disable controlling the behavior of cache-control HTTP 1.1 header values.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable ignoring cache-control HTTP 1.1 header values.</td></tr><tr><td><i>disable</i></td><td>Disable ignoring cache-control HTTP 1.1 header values.</td></tr></table>	Option	Description	<i>enable</i>	Enable ignoring cache-control HTTP 1.1 header values.	<i>disable</i>	Disable ignoring cache-control HTTP 1.1 header values.			
Option	Description									
<i>enable</i>	Enable ignoring cache-control HTTP 1.1 header values.									
<i>disable</i>	Disable ignoring cache-control HTTP 1.1 header values.									
ignore-ie-reload	Enable/disable ignoring the PNC-interpretation of Internet Explorer's Accept: / header.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Enable/disable ignoring the PNC-interpretation of Internet Explorer's Accept: / header.</td></tr><tr><td><i>disable</i></td><td>Disable Enable/disable ignoring the PNC-interpretation of Internet Explorer's Accept: / header.</td></tr></table>	Option	Description	<i>enable</i>	Enable Enable/disable ignoring the PNC-interpretation of Internet Explorer's Accept: / header.	<i>disable</i>	Disable Enable/disable ignoring the PNC-interpretation of Internet Explorer's Accept: / header.			
Option	Description									
<i>enable</i>	Enable Enable/disable ignoring the PNC-interpretation of Internet Explorer's Accept: / header.									
<i>disable</i>	Disable Enable/disable ignoring the PNC-interpretation of Internet Explorer's Accept: / header.									
ignore-ims	Enable/disable ignoring the if-modified-since (IMS) header.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable ignoring the if-modified-since (IMS) header.</td></tr><tr><td><i>disable</i></td><td>Disable ignoring the if-modified-since (IMS) header.</td></tr></table>	Option	Description	<i>enable</i>	Enable ignoring the if-modified-since (IMS) header.	<i>disable</i>	Disable ignoring the if-modified-since (IMS) header.			
Option	Description									
<i>enable</i>	Enable ignoring the if-modified-since (IMS) header.									
<i>disable</i>	Disable ignoring the if-modified-since (IMS) header.									
ignore-pnc	Enable/disable ignoring the pragma no-cache (PNC) header.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable ignoring the pragma no-cache (PNC) header.</td></tr><tr><td><i>disable</i></td><td>Disable ignoring the pragma no-cache (PNC) header.</td></tr></table>	Option	Description	<i>enable</i>	Enable ignoring the pragma no-cache (PNC) header.	<i>disable</i>	Disable ignoring the pragma no-cache (PNC) header.			
Option	Description									
<i>enable</i>	Enable ignoring the pragma no-cache (PNC) header.									
<i>disable</i>	Disable ignoring the pragma no-cache (PNC) header.									

Parameter	Description	Type	Size	Default						
max-object-size	Maximum cacheable object size in kB. All objects that exceed this are delivered to the client but not stored in the web cache.	integer	Minimum value: 1 Maximum value: 2147483	512000						
max-ttl	Maximum time an object can stay in the web cache without checking to see if it has expired on the server.	integer	Minimum value: 1 Maximum value: 5256000	7200						
min-ttl	Minimum time an object can stay in the web cache without checking to see if it has expired on the server.	integer	Minimum value: 1 Maximum value: 5256000	5						
neg-resp-time	Time in minutes to cache negative responses or errors.	integer	Minimum value: 0 Maximum value: 4294967295	0						
reval-pnc	Enable/disable revalidation of pragma-no-cache (PNC) to address bandwidth concerns.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable revalidation of pragma-no-cache (PNC).</td></tr><tr><td><i>disable</i></td><td>Disable revalidation of pragma-no-cache (PNC).</td></tr></table>				Option	Description	<i>enable</i>	Enable revalidation of pragma-no-cache (PNC).	<i>disable</i>	Disable revalidation of pragma-no-cache (PNC).
Option	Description									
<i>enable</i>	Enable revalidation of pragma-no-cache (PNC).									
<i>disable</i>	Disable revalidation of pragma-no-cache (PNC).									

# web-proxy

This section includes syntax for the following commands:

- [config web-proxy debug-url on page 1856](#)
- [config web-proxy explicit on page 1857](#)
- [config web-proxy forward-server-group on page 1862](#)
- [config web-proxy forward-server on page 1863](#)
- [config web-proxy global on page 1865](#)
- [config web-proxy profile on page 1867](#)
- [config web-proxy url-match on page 1872](#)
- [config web-proxy wisp on page 1872](#)

## config web-proxy debug-url

Configure debug URL addresses.

```
config web-proxy debug-url
  Description: Configure debug URL addresses.
  edit <name>
    set exact [enable|disable]
    set status [enable|disable]
    set url-pattern {string}
  next
end
```

## config web-proxy debug-url

Parameter	Description	Type	Size	Default
exact	Enable/disable matching the exact path.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable matching the exact path.		
	<i>disable</i>	Disable matching the exact path.		
name	Debug URL name.	string	Maximum length: 63	
status	Enable/disable this URL exemption.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable this URL exemption.		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>disable</i>	Disable this URL exemption.		
url-pattern	URL exemption pattern.	string	Maximum length: 511	

## config web-proxy explicit

Configure explicit Web proxy settings.

```
config web-proxy explicit
    Description: Configure explicit Web proxy settings.
    set ftp-incoming-port {user}
    set ftp-over-http [enable|disable]
    set http-incoming-port {user}
    set https-incoming-port {user}
    set https-replacement-message [enable|disable]
    set incoming-ip {ipv4-address-any}
    set incoming-ip6 {ipv6-address}
    set ipv6-status [enable|disable]
    set message-upon-server-error [enable|disable]
    set outgoing-ip {ipv4-address-any}
    set outgoing-ip6 {ipv6-address}
    set pac-file-data {user}
    set pac-file-name {string}
    set pac-file-server-port {user}
    set pac-file-server-status [enable|disable]
    set pac-file-url {user}
config pac-policy
    Description: PAC policies.
    edit <policyid>
        set status [enable|disable]
        set srcaddr <name1>, <name2>, ...
        set srcaddr6 <name1>, <name2>, ...
        set dstaddr <name1>, <name2>, ...
        set pac-file-name {string}
        set pac-file-data {user}
        set comments {var-string}
    next
end
set pref-dns-result [ipv4|ipv6]
set realm {string}
set sec-default-action [accept|deny]
set socks [enable|disable]
set socks-incoming-port {user}
set ssl-algorithm [high|medium|...]
set status [enable|disable]
set strict-guest [enable|disable]
set trace-auth-no-rsp [enable|disable]
set unknown-http-version [reject|best-effort]
end
```

## config web-proxy explicit

Parameter	Description	Type	Size	Default						
ftp-incoming-port	Accept incoming FTP-over-HTTP requests on one or more ports.	user	Not Specified							
ftp-over-http	Enable to proxy FTP-over-HTTP sessions sent from a web browser.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable FTP-over-HTTP sessions.</td></tr><tr><td><i>disable</i></td><td>Disable FTP-over-HTTP sessions.</td></tr></table>	Option	Description	<i>enable</i>	Enable FTP-over-HTTP sessions.	<i>disable</i>	Disable FTP-over-HTTP sessions.			
Option	Description									
<i>enable</i>	Enable FTP-over-HTTP sessions.									
<i>disable</i>	Disable FTP-over-HTTP sessions.									
http-incoming-port	Accept incoming HTTP requests on one or more ports.	user	Not Specified							
https-incoming-port	Accept incoming HTTPS requests on one or more ports.	user	Not Specified							
https-replacement-message	Enable/disable sending the client a replacement message for HTTPS requests.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Display a replacement message for HTTPS requests.</td></tr><tr><td><i>disable</i></td><td>Do not display a replacement message for HTTPS requests.</td></tr></table>	Option	Description	<i>enable</i>	Display a replacement message for HTTPS requests.	<i>disable</i>	Do not display a replacement message for HTTPS requests.			
Option	Description									
<i>enable</i>	Display a replacement message for HTTPS requests.									
<i>disable</i>	Do not display a replacement message for HTTPS requests.									
incoming-ip	Restrict the explicit HTTP proxy to only accept sessions from this IP address. An interface must have this IP address.	ipv4-address-any	Not Specified	0.0.0.0						
incoming-ip6	Restrict the explicit web proxy to only accept sessions from this IPv6 address. An interface must have this IPv6 address.	ipv6-address	Not Specified	::						
ipv6-status	Enable/disable allowing an IPv6 web proxy destination in policies and all IPv6 related entries in this command.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable allowing an IPv6 web proxy destination.</td></tr><tr><td><i>disable</i></td><td>Disable allowing an IPv6 web proxy destination.</td></tr></table>	Option	Description	<i>enable</i>	Enable allowing an IPv6 web proxy destination.	<i>disable</i>	Disable allowing an IPv6 web proxy destination.			
Option	Description									
<i>enable</i>	Enable allowing an IPv6 web proxy destination.									
<i>disable</i>	Disable allowing an IPv6 web proxy destination.									
message-upon-server-error	Enable/disable displaying a replacement message when a server error is detected.	option	-	enable						

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Display a replacement message when a server error is detected.		
	<i>disable</i>	Do not display a replacement message when a server error is detected.		
outgoing-ip	Outgoing HTTP requests will have this IP address as their source address. An interface must have this IP address.	ipv4-address-any	Not Specified	
outgoing-ip6	Outgoing HTTP requests will leave this IPv6. Multiple interfaces can be specified. Interfaces must have these IPv6 addresses.	ipv6-address	Not Specified	
pac-file-data	PAC file contents enclosed in quotes (maximum of 256K bytes).	user	Not Specified	
pac-file-name	Pac file name.	string	Maximum length: 63	proxy.pac
pac-file-server-port	Port number that PAC traffic from client web browsers uses to connect to the explicit web proxy.	user	Not Specified	
pac-file-server-status	Enable/disable Proxy Auto-Configuration (PAC) for users of this explicit proxy profile.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable Proxy Auto-Configuration (PAC).		
	<i>disable</i>	Disable Proxy Auto-Configuration (PAC).		
pac-file-url	PAC file access URL.	user	Not Specified	
pref-dns-result	Prefer resolving addresses using the configured IPv4 or IPv6 DNS server.	option	-	ipv4
	<b>Option</b>	<b>Description</b>		
	<i>ipv4</i>	Prefer the IPv4 DNS server.		
	<i>ipv6</i>	Prefer the IPv6 DNS server.		
realm	Authentication realm used to identify the explicit web proxy (maximum of 63 characters).	string	Maximum length: 63	default
sec-default-action	Accept or deny explicit web proxy sessions when no web proxy firewall policy exists.	option	-	deny

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>accept</i>	Accept requests. All explicit web proxy traffic is accepted whether there is an explicit web proxy policy or not.		
	<i>deny</i>	Deny requests unless there is a matching explicit web proxy policy.		
socks	Enable/disable the SOCKS proxy.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable the SOCKS proxy.		
	<i>disable</i>	Disable the SOCKS proxy.		
socks-incoming-port	Accept incoming SOCKS proxy requests on one or more ports.	user	Not Specified	
ssl-algorithm	Relative strength of encryption algorithms accepted in HTTPS deep scan: high, medium, or low.	option	-	low
	<b>Option</b>	<b>Description</b>		
	<i>high</i>	High encryption. Allow only AES and ChaCha.		
	<i>medium</i>	Medium encryption. Allow AES, ChaCha, 3DES, and RC4.		
	<i>low</i>	Low encryption. Allow AES, ChaCha, 3DES, RC4, and DES.		
status	Enable/disable the explicit Web proxy for HTTP and HTTPS session.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable the explicit web proxy.		
	<i>disable</i>	Disable the explicit web proxy.		
strict-guest	Enable/disable strict guest user checking by the explicit web proxy.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable strict guest user checking.		
	<i>disable</i>	Disable strict guest user checking.		
trace-auth-no-rsp	Enable/disable logging timed-out authentication requests.	option	-	disable



Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable logging timed-out authentication requests.		
	<i>disable</i>	Disable logging timed-out authentication requests.		
unknown-http-version	How to handle HTTP sessions that do not comply with HTTP 0.9, 1.0, or 1.1.	option	-	reject
	<b>Option</b>	<b>Description</b>		
	<i>reject</i>	Reject or tear down HTTP sessions that do not use HTTP 0.9, 1.0, or 1.1.		
	<i>best-effort</i>	Assume all HTTP sessions comply with HTTP 0.9, 1.0, or 1.1. If a session uses a different HTTP version, it may not parse correctly and the connection may be lost.		

### config pac-policy

Parameter	Description	Type	Size	Default
policyid	Policy ID.	integer	Minimum value: 1 Maximum value: 100	0
status	Enable/disable policy.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable policy.		
	<i>disable</i>	Disable policy.		
srcaddr <name>	Source address objects. Address name.	string	Maximum length: 79	
srcaddr6 <name>	Source address6 objects. Address name.	string	Maximum length: 79	
dstaddr <name>	Destination address objects. Address name.	string	Maximum length: 79	
pac-file-name	Pac file name.	string	Maximum length: 63	proxy.pac
pac-file-data	PAC file contents enclosed in quotes (maximum of 256K bytes).	user	Not Specified	
comments	Optional comments.	var-string	Maximum length: 1023	

## config web-proxy forward-server-group

Configure a forward server group consisting of multiple forward servers. Supports failover and load balancing.

```
config web-proxy forward-server-group
    Description: Configure a forward server group consisting of multiple forward servers.
    Supports failover and load balancing.
    edit <name>
        set affinity [enable|disable]
        set group-down-option [block|pass]
        set ldb-method [weighted|least-session|...]
        config server-list
            Description: Add web forward servers to a list to form a server group.
            Optionally assign weights to each server.
            edit <name>
                set weight {integer}
            next
        end
    next
end
```

## config web-proxy forward-server-group

Parameter	Description	Type	Size	Default						
affinity	Enable/disable affinity, attaching a source-ip's traffic to the assigned forwarding server until the forward-server-affinity-timeout is reached (under web-proxy global).	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable affinity.</td></tr><tr><td><i>disable</i></td><td>Disable affinity.</td></tr></table>	Option	Description	<i>enable</i>	Enable affinity.	<i>disable</i>	Disable affinity.			
Option	Description									
<i>enable</i>	Enable affinity.									
<i>disable</i>	Disable affinity.									
group-down-option	Action to take when all of the servers in the forward server group are down: block sessions until at least one server is back up or pass sessions to their destination.	option	-	block						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>block</i></td><td>Block sessions until at least one server in the group is back up.</td></tr><tr><td><i>pass</i></td><td>Pass sessions to their destination bypassing servers in the forward server group.</td></tr></table>	Option	Description	<i>block</i>	Block sessions until at least one server in the group is back up.	<i>pass</i>	Pass sessions to their destination bypassing servers in the forward server group.			
Option	Description									
<i>block</i>	Block sessions until at least one server in the group is back up.									
<i>pass</i>	Pass sessions to their destination bypassing servers in the forward server group.									
ldb-method	Load balance method: weighted or least-session.	option	-	weighted						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>weighted</i></td><td>Load balance traffic to forward servers based on assigned weights. Weights are ratios of total number of sessions.</td></tr></table>	Option	Description	<i>weighted</i>	Load balance traffic to forward servers based on assigned weights. Weights are ratios of total number of sessions.					
Option	Description									
<i>weighted</i>	Load balance traffic to forward servers based on assigned weights. Weights are ratios of total number of sessions.									

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>least-session</i>	Send new sessions to the server with lowest session count.		
	<i>active-passive</i>	Send new sessions to the next active server in the list. Servers are selected with highest weight first and then in order as they are configured. Traffic switches back to the first server upon failure recovery.		
name	Configure a forward server group consisting one or multiple forward servers. Supports failover and load balancing.	string	Maximum length: 63	

### config server-list

Parameter	Description	Type	Size	Default
name	Forward server name.	string	Maximum length: 63	
weight	Optionally assign a weight of the forwarding server for weighted load balancing.	integer	Minimum value: 1 Maximum value: 100	10

### config web-proxy forward-server

Configure forward-server addresses.

```

config web-proxy forward-server
    Description: Configure forward-server addresses.
    edit <name>
        set addr-type [ip|fqdn]
        set comment {string}
        set fqdn {string}
        set healthcheck [disable|enable]
        set ip {ipv4-address-any}
        set monitor {string}
        set password {password}
        set port {integer}
        set server-down-option [block|pass]
        set username {string}
    next
end

```

## config web-proxy forward-server

Parameter	Description	Type	Size	Default						
addr-type	Address type of the forwarding proxy server: IP or FQDN.	option	-	ip						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ip</i></td><td>Use an IP address for the forwarding proxy server.</td></tr><tr><td><i>fqdn</i></td><td>Use the FQDN for the forwarding proxy server.</td></tr></table>	Option	Description	<i>ip</i>	Use an IP address for the forwarding proxy server.	<i>fqdn</i>	Use the FQDN for the forwarding proxy server.			
Option	Description									
<i>ip</i>	Use an IP address for the forwarding proxy server.									
<i>fqdn</i>	Use the FQDN for the forwarding proxy server.									
comment	Comment.	string	Maximum length: 63							
fqdn	Forward server Fully Qualified Domain Name (FQDN).	string	Maximum length: 255							
healthcheck	Enable/disable forward server health checking. Attempts to connect through the remote forwarding server to a destination to verify that the forwarding server is operating normally.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable health checking.</td></tr><tr><td><i>enable</i></td><td>Enable health checking.</td></tr></table>	Option	Description	<i>disable</i>	Disable health checking.	<i>enable</i>	Enable health checking.			
Option	Description									
<i>disable</i>	Disable health checking.									
<i>enable</i>	Enable health checking.									
ip	Forward proxy server IP address.	ipv4-address-any	Not Specified	0.0.0.0						
monitor	URL for forward server health check monitoring.	string	Maximum length: 255	http://www.google.com						
name	Server name.	string	Maximum length: 63							
password	HTTP authentication password.	password	Not Specified							
port	Port number that the forwarding server expects to receive HTTP sessions on.	integer	Minimum value: 1 Maximum value: 65535	3128						
server-down-option	Action to take when the forward server is found to be down: block sessions until the server is back up or pass sessions to their destination.	option	-	block						

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>block</i>	Block sessions until the server is back up.		
	<i>pass</i>	Pass sessions to their destination bypassing the forward server.		
username	HTTP authentication user name.	string	Maximum length: 64	

## config web-proxy global

Configure Web proxy global settings.

```
config web-proxy global
    Description: Configure Web proxy global settings.
    set fast-policy-match [enable|disable]
    set forward-proxy-auth [enable|disable]
    set forward-server-affinity-timeout {integer}
    set ldap-user-cache [enable|disable]
    set learn-client-ip [enable|disable]
    set learn-client-ip-from-header {option1}, {option2}, ...
    set learn-client-ip-srcaddr <name1>, <name2>, ...
    set learn-client-ip-srcaddr6 <name1>, <name2>, ...
    set max-message-length {integer}
    set max-request-length {integer}
    set max-waf-body-cache-length {integer}
    set proxy-fqdn {string}
    set src-affinity-exempt-addr {ipv4-address-any}
    set src-affinity-exempt-addr6 {ipv6-address}
    set ssl-ca-cert {string}
    set ssl-cert {string}
    set strict-web-check [enable|disable]
    set webproxy-profile {string}
end
```

## config web-proxy global

Parameter	Description	Type	Size	Default
fast-policy-match	Enable/disable fast matching algorithm for explicit and transparent proxy policy.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
forward-proxy-auth	Enable/disable forwarding proxy authentication headers.	option	-	disable

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable forwarding proxy authentication headers.		
	<i>disable</i>	Disable forwarding proxy authentication headers.		
forward-server-affinity-timeout	Period of time before the source IP's traffic is no longer assigned to the forwarding server.	integer	Minimum value: 6 Maximum value: 60	30
ldap-user-cache	Enable/disable LDAP user cache for explicit and transparent proxy user.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
learn-client-ip	Enable/disable learning the client's IP address from headers.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable learning the client's IP address from headers.		
	<i>disable</i>	Disable learning the client's IP address from headers.		
learn-client-ip-from-header	Learn client IP address from the specified headers.	option	-	
	<b>Option</b>	<b>Description</b>		
	<i>true-client-ip</i>	Learn the client IP address from the True-Client-IP header.		
	<i>x-real-ip</i>	Learn the client IP address from the X-Real-IP header.		
	<i>x-forwarded-for</i>	Learn the client IP address from the X-Forwarded-For header.		
learn-client-ip-srcaddr <name>	Source address name (srcaddr or srcaddr6 must be set). Address name.	string	Maximum length: 79	
learn-client-ip-srcaddr6 <name>	IPv6 Source address name (srcaddr or srcaddr6 must be set). Address name.	string	Maximum length: 79	
max-message-length	Maximum length of HTTP message, not including body.	integer	Minimum value: 16 Maximum value: 256	32

Parameter	Description	Type	Size	Default						
max-request-length	Maximum length of HTTP request line.	integer	Minimum value: 2 Maximum value: 64	8						
max-waf-body-cache-length	Maximum length of HTTP messages processed by Web Application Firewall.	integer	Minimum value: 10 Maximum value: 1024	32						
proxy-fqdn	Fully Qualified Domain Name to connect to the explicit web proxy.	string	Maximum length: 255	default.fqdn						
src-affinity-exempt-addr	IPv4 source addresses to exempt proxy affinity.	ipv4-address-any	Not Specified							
src-affinity-exempt-addr6	IPv6 source addresses to exempt proxy affinity.	ipv6-address	Not Specified							
ssl-ca-cert	SSL CA certificate for SSL interception.	string	Maximum length: 35	Fortinet_CA_SSL						
ssl-cert	SSL certificate for SSL interception.	string	Maximum length: 35	Fortinet_Factory						
strict-web-check	Enable/disable strict web checking to block web sites that send incorrect headers that don't conform to HTTP 1.1.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable strict web checking.</td></tr><tr><td><i>disable</i></td><td>Disable strict web checking.</td></tr></table>				Option	Description	<i>enable</i>	Enable strict web checking.	<i>disable</i>	Disable strict web checking.
Option	Description									
<i>enable</i>	Enable strict web checking.									
<i>disable</i>	Disable strict web checking.									
webproxy-profile	Name of the web proxy profile to apply when explicit proxy traffic is allowed by default and traffic is accepted that does not match an explicit proxy policy.	string	Maximum length: 63							

## config web-proxy profile

Configure web proxy profiles.

```
config web-proxy profile
  Description: Configure web proxy profiles.
  edit <name>
    set header-client-ip [pass|add|...]
    set header-front-end-https [pass|add|...]
    set header-via-request [pass|add|...]
    set header-via-response [pass|add|...]
    set header-x-authenticated-groups [pass|add|...]
    set header-x-authenticated-user [pass|add|...]
```

```

set header-x-forwarded-client-cert [pass|add|...]
set header-x-forwarded-for [pass|add|...]
config headers
    Description: Configure HTTP forwarded requests headers.
    edit <id>
        set name {string}
        set dstaddr <name1>, <name2>, ...
        set dstaddr6 <name1>, <name2>, ...
        set action [add-to-request|add-to-response|...]
        set content {string}
        set base64-encoding [disable|enable]
        set add-option [append|new-on-not-found|...]
        set protocol {option1}, {option2}, ...
    next
end
set log-header-change [enable|disable]
set strip-encoding [enable|disable]
next
end

```

## config web-proxy profile

Parameter	Description	Type	Size	Default								
header-client-ip	Action to take on the HTTP client-IP header in forwarded requests: forwards (pass), adds, or removes the HTTP header.	option	-	pass								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>pass</i></td><td>Forward the same HTTP header.</td></tr><tr><td><i>add</i></td><td>Add the HTTP header.</td></tr><tr><td><i>remove</i></td><td>Remove the HTTP header.</td></tr></table>	Option	Description	<i>pass</i>	Forward the same HTTP header.	<i>add</i>	Add the HTTP header.	<i>remove</i>	Remove the HTTP header.			
Option	Description											
<i>pass</i>	Forward the same HTTP header.											
<i>add</i>	Add the HTTP header.											
<i>remove</i>	Remove the HTTP header.											
header-front-end-https	Action to take on the HTTP front-end-HTTPS header in forwarded requests: forwards (pass), adds, or removes the HTTP header.	option	-	pass								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>pass</i></td><td>Forward the same HTTP header.</td></tr><tr><td><i>add</i></td><td>Add the HTTP header.</td></tr><tr><td><i>remove</i></td><td>Remove the HTTP header.</td></tr></table>	Option	Description	<i>pass</i>	Forward the same HTTP header.	<i>add</i>	Add the HTTP header.	<i>remove</i>	Remove the HTTP header.			
Option	Description											
<i>pass</i>	Forward the same HTTP header.											
<i>add</i>	Add the HTTP header.											
<i>remove</i>	Remove the HTTP header.											
header-via-request	Action to take on the HTTP via header in forwarded requests: forwards (pass), adds, or removes the HTTP header.	option	-	pass								



Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>pass</i>	Forward the same HTTP header.		
	<i>add</i>	Add the HTTP header.		
	<i>remove</i>	Remove the HTTP header.		
header-via-response	Action to take on the HTTP via header in forwarded responses: forwards (pass), adds, or removes the HTTP header.	option	-	pass
	<b>Option</b>	<b>Description</b>		
	<i>pass</i>	Forward the same HTTP header.		
	<i>add</i>	Add the HTTP header.		
	<i>remove</i>	Remove the HTTP header.		
header-x-authenticated-groups	Action to take on the HTTP x-authenticated-groups header in forwarded requests: forwards (pass), adds, or removes the HTTP header.	option	-	pass
	<b>Option</b>	<b>Description</b>		
	<i>pass</i>	Forward the same HTTP header.		
	<i>add</i>	Add the HTTP header.		
	<i>remove</i>	Remove the HTTP header.		
header-x-authenticated-user	Action to take on the HTTP x-authenticated-user header in forwarded requests: forwards (pass), adds, or removes the HTTP header.	option	-	pass
	<b>Option</b>	<b>Description</b>		
	<i>pass</i>	Forward the same HTTP header.		
	<i>add</i>	Add the HTTP header.		
	<i>remove</i>	Remove the HTTP header.		
header-x-forwarded-client-cert	Action to take on the HTTP x-forwarded-client-cert header in forwarded requests: forwards (pass), adds, or removes the HTTP header.	option	-	pass
	<b>Option</b>	<b>Description</b>		
	<i>pass</i>	Forward the same HTTP header.		

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>add</i></td><td>Add the HTTP header.</td></tr><tr><td><i>remove</i></td><td>Remove the HTTP header.</td></tr></table>	Option	Description	<i>add</i>	Add the HTTP header.	<i>remove</i>	Remove the HTTP header.					
	Option	Description										
	<i>add</i>	Add the HTTP header.										
<i>remove</i>	Remove the HTTP header.											
header-x-forwarded-for	Action to take on the HTTP x-forwarded-for header in forwarded requests: forwards (pass), adds, or removes the HTTP header.	option	-	pass								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>pass</i></td><td>Forward the same HTTP header.</td></tr><tr><td><i>add</i></td><td>Add the HTTP header.</td></tr><tr><td><i>remove</i></td><td>Remove the HTTP header.</td></tr></table>	Option	Description	<i>pass</i>	Forward the same HTTP header.	<i>add</i>	Add the HTTP header.	<i>remove</i>	Remove the HTTP header.			
	Option	Description										
	<i>pass</i>	Forward the same HTTP header.										
	<i>add</i>	Add the HTTP header.										
<i>remove</i>	Remove the HTTP header.											
log-header-change	Enable/disable logging HTTP header changes.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Enable/disable logging HTTP header changes.</td></tr><tr><td><i>disable</i></td><td>Disable Enable/disable logging HTTP header changes.</td></tr></table>	Option	Description	<i>enable</i>	Enable Enable/disable logging HTTP header changes.	<i>disable</i>	Disable Enable/disable logging HTTP header changes.					
	Option	Description										
	<i>enable</i>	Enable Enable/disable logging HTTP header changes.										
<i>disable</i>	Disable Enable/disable logging HTTP header changes.											
name	Profile name.	string	Maximum length: 63									
strip-encoding	Enable/disable stripping unsupported encoding from the request header.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable stripping of unsupported encoding from the request header.</td></tr><tr><td><i>disable</i></td><td>Disable stripping of unsupported encoding from the request header.</td></tr></table>	Option	Description	<i>enable</i>	Enable stripping of unsupported encoding from the request header.	<i>disable</i>	Disable stripping of unsupported encoding from the request header.					
	Option	Description										
	<i>enable</i>	Enable stripping of unsupported encoding from the request header.										
<i>disable</i>	Disable stripping of unsupported encoding from the request header.											

## config headers

Parameter	Description	Type	Size	Default
id	HTTP forwarded header id.	integer	Minimum value: 0 Maximum value: 4294967295	0
name	HTTP forwarded header name.	string	Maximum length: 79	

Parameter	Description	Type	Size	Default										
dstaddr <name>	Destination address and address group names. Address name.	string	Maximum length: 79											
dstaddr6 <name>	Destination address and address group names (IPv6). Address name.	string	Maximum length: 79											
action	Action when the HTTP header is forwarded.	option	-	add-to-request										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>add-to-request</td><td>Add the HTTP header to request.</td></tr><tr><td>add-to-response</td><td>Add the HTTP header to response.</td></tr><tr><td>remove-from-request</td><td>Remove the HTTP header from request.</td></tr><tr><td>remove-from-response</td><td>Remove the HTTP header from response.</td></tr></table>				Option	Description	add-to-request	Add the HTTP header to request.	add-to-response	Add the HTTP header to response.	remove-from-request	Remove the HTTP header from request.	remove-from-response	Remove the HTTP header from response.
Option	Description													
add-to-request	Add the HTTP header to request.													
add-to-response	Add the HTTP header to response.													
remove-from-request	Remove the HTTP header from request.													
remove-from-response	Remove the HTTP header from response.													
content	HTTP header content.	string	Maximum length: 1023											
base64-encoding	Enable/disable use of base64 encoding of HTTP content.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable use of base64 encoding of HTTP content.</td></tr><tr><td>enable</td><td>Enable use of base64 encoding of HTTP content.</td></tr></table>				Option	Description	disable	Disable use of base64 encoding of HTTP content.	enable	Enable use of base64 encoding of HTTP content.				
Option	Description													
disable	Disable use of base64 encoding of HTTP content.													
enable	Enable use of base64 encoding of HTTP content.													
add-option	Configure options to append content to existing HTTP header or add new HTTP header.	option	-	new										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>append</td><td>Append content to existing HTTP header or create new header if HTTP header is not found.</td></tr><tr><td>new-on-not-found</td><td>Create new header only if existing HTTP header is not found.</td></tr><tr><td>new</td><td>Create new header regardless if existing HTTP header is found or not.</td></tr></table>				Option	Description	append	Append content to existing HTTP header or create new header if HTTP header is not found.	new-on-not-found	Create new header only if existing HTTP header is not found.	new	Create new header regardless if existing HTTP header is found or not.		
Option	Description													
append	Append content to existing HTTP header or create new header if HTTP header is not found.													
new-on-not-found	Create new header only if existing HTTP header is not found.													
new	Create new header regardless if existing HTTP header is found or not.													
protocol	Configure protocol(s) to take add-option action on (HTTP, HTTPS, or both).	option	-	https http										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>https</td><td>Perform add-option action on HTTPS.</td></tr><tr><td>http</td><td>Perform add-option action on HTTP.</td></tr></table>				Option	Description	https	Perform add-option action on HTTPS.	http	Perform add-option action on HTTP.				
Option	Description													
https	Perform add-option action on HTTPS.													
http	Perform add-option action on HTTP.													

## config web-proxy url-match

Exempt URLs from web proxy forwarding and caching.

```
config web-proxy url-match
  Description: Exempt URLs from web proxy forwarding and caching.
  edit <name>
    set cache-exemption [enable|disable]
    set comment {var-string}
    set forward-server {string}
    set status [enable|disable]
    set url-pattern {string}
  next
end
```

## config web-proxy url-match

Parameter	Description	Type	Size	Default
cache-exemption	Enable/disable exempting this URL pattern from caching.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable exempting this URL pattern from caching.		
	<i>disable</i>	Disable exempting this URL pattern from caching.		
comment	Comment.	var-string	Maximum length: 255	
forward-server	Forward server name.	string	Maximum length: 63	
name	Configure a name for the URL to be exempted.	string	Maximum length: 63	
status	Enable/disable exempting the URLs matching the URL pattern from web proxy forwarding and caching.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable exempting the matching URLs.		
	<i>disable</i>	Disable exempting the matching URLs.		
url-pattern	URL pattern to be exempted from web proxy forwarding and caching.	string	Maximum length: 511	

## config web-proxy wisp

Configure Websense Integrated Services Protocol (WISP) servers.

```

config web-proxy wisp
    Description: Configure Websense Integrated Services Protocol (WISP) servers.
    edit <name>
        set comment {var-string}
        set max-connections {integer}
        set outgoing-ip {ipv4-address-any}
        set server-ip {ipv4-address-any}
        set server-port {integer}
        set timeout {integer}
    next
end

```

## config web-proxy wisp

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 255	
max-connections	Maximum number of web proxy WISP connections.	integer	Minimum value: 4 Maximum value: 4096	64
name	Server name.	string	Maximum length: 35	
outgoing-ip	WISP outgoing IP address.	ipv4-address-any	Not Specified	0.0.0.0
server-ip	WISP server IP address.	ipv4-address-any	Not Specified	0.0.0.0
server-port	WISP server port.	integer	Minimum value: 1 Maximum value: 65535	15868
timeout	Period of time before WISP requests time out.	integer	Minimum value: 1 Maximum value: 15	5

## webfilter

This section includes syntax for the following commands:

- [config webfilter content-header on page 1874](#)
- [config webfilter content on page 1875](#)
- [config webfilter fortiguard on page 1877](#)
- [config webfilter ftgd-local-cat on page 1879](#)
- [config webfilter ftgd-local-rating on page 1880](#)
- [config webfilter ips-urlfilter-cache-setting on page 1881](#)
- [config webfilter ips-urlfilter-setting on page 1881](#)
- [config webfilter ips-urlfilter-setting6 on page 1882](#)
- [config webfilter override on page 1882](#)
- [config webfilter profile on page 1884](#)
- [config webfilter search-engine on page 1901](#)
- [config webfilter urlfilter on page 1903](#)

### config webfilter content-header

Configure content types used by Web filter.

```
config webfilter content-header
  Description: Configure content types used by Web filter.
  edit <id>
    set comment {var-string}
    config entries
      Description: Configure content types used by web filter.
      edit <pattern>
        set action [block|allow|...]
        set category {user}
      next
    end
    set name {string}
  next
end
```

### config webfilter content-header

Parameter	Description	Type	Size	Default
comment	Optional comments.	var-string	Maximum length: 255	

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
name	Name of table.	string	Maximum length: 63	

### config entries

Parameter	Description	Type	Size	Default								
pattern	Content type (regular expression).	string	Maximum length: 31									
action	Action to take for this content type.	option	-	allow								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>block</i></td><td>Block content type.</td></tr><tr><td><i>allow</i></td><td>Allow content type.</td></tr><tr><td><i>exempt</i></td><td>Exempt content type.</td></tr></table>				Option	Description	<i>block</i>	Block content type.	<i>allow</i>	Allow content type.	<i>exempt</i>	Exempt content type.
	Option	Description										
	<i>block</i>	Block content type.										
	<i>allow</i>	Allow content type.										
<i>exempt</i>	Exempt content type.											
category	Categories that this content type applies to.	user	Not Specified	all								

### config webfilter content

Configure Web filter banned word table.

```

config webfilter content
    Description: Configure Web filter banned word table.
    edit <id>
        set comment {var-string}
        config entries
            Description: Configure banned word entries.
            edit <name>
                set pattern-type [wildcard|regexp]
                set status [enable|disable]
                set lang [western|simch|...]
                set score {integer}
                set action [block|exempt]
            next
        end
        set name {string}
    next
end

```

## config webfilter content

Parameter	Description	Type	Size	Default
comment	Optional comments.	var-string	Maximum length: 255	
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
name	Name of table.	string	Maximum length: 63	

## config entries

Parameter	Description	Type	Size	Default
name	Banned word.	string	Maximum length: 127	
pattern-type	Banned word pattern type: wildcard pattern or Perl regular expression.	option	-	wildcard
	<b>Option</b>	<b>Description</b>		
	wildcard	Wildcard pattern.		
	regex	Perl regular expression.		
status	Enable/disable banned word.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	enable	Enable setting.		
	disable	Disable setting.		
lang	Language of banned word.	option	-	western
	<b>Option</b>	<b>Description</b>		
	western	Western.		
	simch	Simplified Chinese.		
	trach	Traditional Chinese.		
	japanese	Japanese.		
	korean	Korean.		



Parameter	Description	Type	Size	Default										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>french</i></td><td>French.</td></tr><tr><td><i>thai</i></td><td>Thai.</td></tr><tr><td><i>spanish</i></td><td>Spanish.</td></tr><tr><td><i>cyrillic</i></td><td>Cyrillic.</td></tr></table>	Option	Description	<i>french</i>	French.	<i>thai</i>	Thai.	<i>spanish</i>	Spanish.	<i>cyrillic</i>	Cyrillic.			
	Option	Description												
	<i>french</i>	French.												
	<i>thai</i>	Thai.												
	<i>spanish</i>	Spanish.												
<i>cyrillic</i>	Cyrillic.													
score	Score, to be applied every time the word appears on a web page.	integer	Minimum value: 0 Maximum value: 4294967295	10										
action	Block or exempt word when a match is found.	option	-	block										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>block</i></td><td>Block matches.</td></tr><tr><td><i>exempt</i></td><td>Exempt matches.</td></tr></table>	Option	Description	<i>block</i>	Block matches.	<i>exempt</i>	Exempt matches.							
	Option	Description												
	<i>block</i>	Block matches.												
<i>exempt</i>	Exempt matches.													

## config webfilter fortiguard

Configure FortiGuard Web Filter service.

```

config webfilter fortiguard
    Description: Configure FortiGuard Web Filter service.
    set cache-mem-percent {integer}
    set cache-mode [ttl|db-ver]
    set cache-prefix-match [enable|disable]
    set close-ports [enable|disable]
    set ovrd-auth-https [enable|disable]
    set ovrd-auth-port-http {integer}
    set ovrd-auth-port-https {integer}
    set ovrd-auth-port-https-flow {integer}
    set ovrd-auth-port-warning {integer}
    set request-packet-size-limit {integer}
    set warn-auth-https [enable|disable]
end

```

## config webfilter fortiguard

Parameter	Description	Type	Size	Default
cache-mem-percent	Maximum percentage of available memory allocated to caching.	integer	Minimum value: 1 Maximum value: 15	2 **
cache-mode	Cache entry expiration mode.	option	-	tll
	<b>Option</b> <b>Description</b>			
	<i>tll</i>	Expire cache items by time-to-live.		
	<i>db-ver</i>	Expire cache items when the server DB version changes.		
cache-prefix-match	Enable/disable prefix matching in the cache.	option	-	enable
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
close-ports	Close ports used for HTTP/HTTPS override authentication and disable user overrides.	option	-	disable
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
ovrd-auth-https	Enable/disable use of HTTPS for override authentication.	option	-	enable
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
ovrd-auth-port-http	Port to use for FortiGuard Web Filter HTTP override authentication.	integer	Minimum value: 0 Maximum value: 65535	8008

Parameter	Description	Type	Size	Default
ovrd-auth-port-https	Port to use for FortiGuard Web Filter HTTPS override authentication in proxy mode.	integer	Minimum value: 0 Maximum value: 65535	8010
ovrd-auth-port-https-flow	Port to use for FortiGuard Web Filter HTTPS override authentication in flow mode.	integer	Minimum value: 0 Maximum value: 65535	8015
ovrd-auth-port-warning	Port to use for FortiGuard Web Filter Warning override authentication.	integer	Minimum value: 0 Maximum value: 65535	8020
request-packet-size-limit	Limit size of URL request packets sent to FortiGuard server.	integer	Minimum value: 576 Maximum value: 10000	0
warn-auth-https	Enable/disable use of HTTPS for warning and authentication.	option	-	enable
		Option	Description	
		<i>enable</i>	Enable setting.	
		<i>disable</i>	Disable setting.	

\*\* Values may differ between models.

## config webfilter ftgd-local-cat

Configure FortiGuard Web Filter local categories.

```
config webfilter ftgd-local-cat
    Description: Configure FortiGuard Web Filter local categories.
    edit <desc>
        set id {integer}
        set status [enable|disable]
    next
end
```

## config webfilter ftgd-local-cat

Parameter	Description	Type	Size	Default						
desc	Local category description.	string	Maximum length: 79							
id	Local category ID.	integer	Minimum value: 140 Maximum value: 191	0						
status	Enable/disable the local category.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable the local category.</td></tr><tr><td><i>disable</i></td><td>Disable the local category.</td></tr></table>				Option	Description	<i>enable</i>	Enable the local category.	<i>disable</i>	Disable the local category.
Option	Description									
<i>enable</i>	Enable the local category.									
<i>disable</i>	Disable the local category.									

## config webfilter ftgd-local-rating

Configure local FortiGuard Web Filter local ratings.

```
config webfilter ftgd-local-rating
  Description: Configure local FortiGuard Web Filter local ratings.
  edit <url>
    set comment {var-string}
    set rating {user}
    set status [enable|disable]
  next
end
```

## config webfilter ftgd-local-rating

Parameter	Description	Type	Size	Default						
comment	Comment.	var-string	Maximum length: 255							
rating	Local rating.	user	Not Specified							
status	Enable/disable local rating.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable local rating.</td></tr><tr><td><i>disable</i></td><td>Disable local rating.</td></tr></table>				Option	Description	<i>enable</i>	Enable local rating.	<i>disable</i>	Disable local rating.
	Option	Description								
	<i>enable</i>	Enable local rating.								
<i>disable</i>	Disable local rating.									
url	URL to rate locally.	string	Maximum length: 511							

## config webfilter ips-urlfilter-cache-setting

Configure IPS URL filter cache settings.

```
config webfilter ips-urlfilter-cache-setting
    Description: Configure IPS URL filter cache settings.
    set dns-retry-interval {integer}
    set extended-ttl {integer}
end
```

## config webfilter ips-urlfilter-cache-setting

Parameter	Description	Type	Size	Default
dns-retry-interval	Retry interval. Refresh DNS faster than TTL to capture multiple IPs for hosts. 0 means use DNS server's TTL only.	integer	Minimum value: 0 Maximum value: 2147483	0
extended-ttl	Extend time to live beyond reported by DNS. Use of 0 means use DNS server's TTL.	integer	Minimum value: 0 Maximum value: 2147483	0

## config webfilter ips-urlfilter-setting

Configure IPS URL filter settings.

```
config webfilter ips-urlfilter-setting
    Description: Configure IPS URL filter settings.
    set device {string}
    set distance {integer}
    set gateway {ipv4-address}
    set geo-filter {var-string}
end
```

## config webfilter ips-urlfilter-setting

Parameter	Description	Type	Size	Default
device	Interface for this route.	string	Maximum length: 35	
distance	Administrative distance for this route.	integer	Minimum value: 1 Maximum value: 255	1

Parameter	Description	Type	Size	Default
gateway	Gateway IP address for this route.	ipv4-address	Not Specified	0.0.0.0
geo-filter	Filter based on geographical location. Route will NOT be installed if the resolved IP address belongs to the country in the filter.	var-string	Maximum length: 255	

## config webfilter ips-urlfilter-setting6

Configure IPS URL filter settings for IPv6.

```
config webfilter ips-urlfilter-setting6
    Description: Configure IPS URL filter settings for IPv6.
    set device {string}
    set distance {integer}
    set gateway6 {ipv6-address}
    set geo-filter {var-string}
end
```

## config webfilter ips-urlfilter-setting6

Parameter	Description	Type	Size	Default
device	Interface for this route.	string	Maximum length: 35	
distance	Administrative distance for this route.	integer	Minimum value: 1 Maximum value: 255	1
gateway6	Gateway IPv6 address for this route.	ipv6-address	Not Specified	::
geo-filter	Filter based on geographical location. Route will NOT be installed if the resolved IPv6 address belongs to the country in the filter.	var-string	Maximum length: 255	

## config webfilter override

Configure FortiGuard Web Filter administrative overrides.

```
config webfilter override
    Description: Configure FortiGuard Web Filter administrative overrides.
    edit <id>
        set expires {user}
        set initiator {string}
        set ip {ipv4-address}
        set ip6 {ipv6-address}
```

```

        set new-profile {string}
        set old-profile {string}
        set scope [user|user-group|...]
        set status [enable|disable]
        set user {string}
        set user-group {string}
    next
end

```

## config webfilter override

Parameter	Description	Type	Size	Default										
expires	Override expiration date and time, from 5 minutes to 365 from now (format: yyyy/mm/dd hh:mm:ss).	user	Not Specified	1969/12/31 17:00:00										
id	Override rule ID.	integer	Minimum value: 0 Maximum value: 4294967295	0										
initiator	Initiating user of override (read-only setting).	string	Maximum length: 64											
ip	IPv4 address which the override applies.	ipv4-address	Not Specified	0.0.0.0										
ip6	IPv6 address which the override applies.	ipv6-address	Not Specified	::										
new-profile	Name of the new web filter profile used by the override.	string	Maximum length: 35											
old-profile	Name of the web filter profile which the override applies.	string	Maximum length: 35											
scope	Override either the specific user, user group, IPv4 address, or IPv6 address.	option	-	user										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>user</td><td>Override the specified user.</td></tr><tr><td>user-group</td><td>Override the specified user group.</td></tr><tr><td>ip</td><td>Override the specified IP address.</td></tr><tr><td>ip6</td><td>Override the specified IPv6 address.</td></tr></table>				Option	Description	user	Override the specified user.	user-group	Override the specified user group.	ip	Override the specified IP address.	ip6	Override the specified IPv6 address.
	Option	Description												
	user	Override the specified user.												
	user-group	Override the specified user group.												
	ip	Override the specified IP address.												
ip6	Override the specified IPv6 address.													
status	Enable/disable override rule.	option	-	disable										

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable override rule.		
	<i>disable</i>	Disable override rule.		
user	Name of the user which the override applies.	string	Maximum length: 64	
user-group	Specify the user group for which the override applies.	string	Maximum length: 63	

## config webfilter profile

Configure Web filter profiles.

```

config webfilter profile
    Description: Configure Web filter profiles.
    edit <name>
        config antiphish
            Description: AntiPhishing profile.
            set status [enable|disable]
            set default-action [exempt|log|...]
            set check-uri [enable|disable]
            set check-basic-auth [enable|disable]
            set check-username-only [enable|disable]
            set max-body-len {integer}
            config inspection-entries
                Description: AntiPhishing entries.
                edit <name>
                    set fortiguard-category {user}
                    set action [exempt|log|...]
                next
            end
            config custom-patterns
                Description: Custom username and password regex patterns.
                edit <pattern>
                    set category [username|password]
                    set type [regex|literal]
                next
            end
            set authentication [domain-controller|ldap]
            set domain-controller {string}
            set ldap {string}
        end
        set comment {var-string}
        set extended-log [enable|disable]
        set feature-set [flow|proxy]
        config ftgd-wf
            Description: FortiGuard Web Filter settings.
            set options {option1}, {option2}, ...
            set exempt-quota {user}
            set ovrd {user}
    
```



```

config filters
    Description: FortiGuard filters.
    edit <id>
        set category {integer}
        set action [block|authenticate|...]
        set warn-duration {user}
        set auth-usr-grp <name1>, <name2>, ...
        set log [enable|disable]
        set override-replacemsg {string}
        set warning-prompt [per-domain|per-category]
        set warning-duration-type [session|timeout]
    next
end
config quota
    Description: FortiGuard traffic quota settings.
    edit <id>
        set category {user}
        set type [time|traffic]
        set unit [B|KB|...]
        set value {integer}
        set duration {user}
        set override-replacemsg {string}
    next
end
set max-quota-timeout {integer}
set rate-javascript-urls [disable|enable]
set rate-css-urls [disable|enable]
set rate-crl-urls [disable|enable]
end
set https-replacemsg [enable|disable]
set log-all-url [enable|disable]
set options {option1}, {option2}, ...
config override
    Description: Web Filter override settings.
    set ovr-d-cookie [allow|deny]
    set ovr-d-scope [user|user-group|...]
    set profile-type [list|radius]
    set ovr-dur-mode [constant|ask]
    set ovr-dur {user}
    set profile-attribute [User-Name|NAS-IP-Address|...]
    set ovr-d-user-group <name1>, <name2>, ...
    set profile <name1>, <name2>, ...
end
set ovr-d-perm {option1}, {option2}, ...
set post-action [normal|block]
set replacemsg-group {string}
config url-extraction
    Description: Configure URL Extraction
    set status [enable|disable]
    set server-fqdn {string}
    set redirect-header {string}
    set redirect-url {string}
    set redirect-no-content [enable|disable]
end
config web
    Description: Web content filtering settings.

```

```

        set bword-threshold {integer}
        set bword-table {integer}
        set urlfilter-table {integer}
        set content-header-list {integer}
        set blocklist [enable|disable]
        set allowlist {option1}, {option2}, ...
        set safe-search {option1}, {option2}, ...
        set youtube-restrict [none|strict|...]
        set vimeo-restrict {string}
        set log-search [enable|disable]
        set keyword-match <pattern1>, <pattern2>, ...
    end
    set web-antiphishing-log [enable|disable]
    set web-content-log [enable|disable]
    set web-extended-all-action-log [enable|disable]
    set web-filter-activex-log [enable|disable]
    set web-filter-applet-log [enable|disable]
    set web-filter-command-block-log [enable|disable]
    set web-filter-cookie-log [enable|disable]
    set web-filter-cookie-removal-log [enable|disable]
    set web-filter-js-log [enable|disable]
    set web-filter-jscript-log [enable|disable]
    set web-filter-referer-log [enable|disable]
    set web-filter-unknown-log [enable|disable]
    set web-filter-vbs-log [enable|disable]
    set web-ftgd-err-log [enable|disable]
    set web-ftgd-quota-usage [enable|disable]
    set web-invalid-domain-log [enable|disable]
    set web-url-log [enable|disable]
    set wisp [enable|disable]
    set wisp-algorithm [primary-secondary|round-robin|...]
    set wisp-servers <name1>, <name2>, ...
next
end

```

## config webfilter profile

Parameter	Description	Type	Size	Default
comment	Optional comments.	var-string	Maximum length: 255	
extended-log	Enable/disable extended logging for web filtering.	option	-	disable
	Option	Description		
	enable	Enable setting.		
	disable	Disable setting.		
feature-set	Flow/proxy feature set.	option	-	flow

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>flow</i>	Flow feature set.		
	<i>proxy</i>	Proxy feature set.		
https-replacemsg	Enable replacement messages for HTTPS.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
log-all-url	Enable/disable logging all URLs visited.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
name	Profile name.	string	Maximum length: 35	
options	Options.	option	-	
	<b>Option</b>	<b>Description</b>		
	<i>activexfilter</i>	ActiveX filter.		
	<i>cookiefilter</i>	Cookie filter.		
	<i>javafilter</i>	Java applet filter.		
	<i>block-invalid-url</i>	Block sessions contained an invalid domain name.		
	<i>jscript</i>	Javascript block.		
	<i>js</i>	JS block.		
	<i>vbs</i>	VB script block.		
	<i>unknown</i>	Unknown script block.		
	<i>intrinsic</i>	Intrinsic script block.		
	<i>wf-referer</i>	Referring block.		
	<i>wf-cookie</i>	Cookie block.		
	<i>per-user-bal</i>	Per-user block/allow list filter		
ovrd-perm	Permitted override types.	option	-	

Parameter	Description	Type	Size	Default										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>bannedword-override</i></td><td>Banned word override.</td></tr><tr><td><i>urlfilter-override</i></td><td>URL filter override.</td></tr><tr><td><i>fortiguard-wf-override</i></td><td>FortiGuard Web Filter override.</td></tr><tr><td><i>contenttype-check-override</i></td><td>Content-type header override.</td></tr></table>	Option	Description	<i>bannedword-override</i>	Banned word override.	<i>urlfilter-override</i>	URL filter override.	<i>fortiguard-wf-override</i>	FortiGuard Web Filter override.	<i>contenttype-check-override</i>	Content-type header override.			
	Option	Description												
	<i>bannedword-override</i>	Banned word override.												
	<i>urlfilter-override</i>	URL filter override.												
	<i>fortiguard-wf-override</i>	FortiGuard Web Filter override.												
<i>contenttype-check-override</i>	Content-type header override.													
post-action	Action taken for HTTP POST traffic.	option	-	normal										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>normal</i></td><td>Normal, POST requests are allowed.</td></tr><tr><td><i>block</i></td><td>POST requests are blocked.</td></tr></table>	Option	Description	<i>normal</i>	Normal, POST requests are allowed.	<i>block</i>	POST requests are blocked.							
	Option	Description												
	<i>normal</i>	Normal, POST requests are allowed.												
<i>block</i>	POST requests are blocked.													
replacemsg-group	Replacement message group.	string	Maximum length: 35											
web-antiphishing-log	Enable/disable logging of AntiPhishing checks.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.							
	Option	Description												
	<i>enable</i>	Enable setting.												
<i>disable</i>	Disable setting.													
web-content-log	Enable/disable logging logging blocked web content.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.							
	Option	Description												
	<i>enable</i>	Enable setting.												
<i>disable</i>	Disable setting.													
web-extended-all-action-log	Enable/disable extended any filter action logging for web filtering.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.							
	Option	Description												
	<i>enable</i>	Enable setting.												
<i>disable</i>	Disable setting.													

Parameter	Description	Type	Size	Default						
web-filter-activex-log	Enable/disable logging ActiveX.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
web-filter-applet-log	Enable/disable logging Java applets.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
web-filter-command-block-log	Enable/disable logging blocked commands.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
web-filter-cookie-log	Enable/disable logging cookie filtering.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
web-filter-cookie-removal-log	Enable/disable logging blocked cookies.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
web-filter-js-log	Enable/disable logging Java scripts.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.					
Option	Description									
<i>enable</i>	Enable setting.									

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable setting.		
web-filter-jscript-log	Enable/disable logging JScripts.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
web-filter-referer-log	Enable/disable logging referrers.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
web-filter-unknown-log	Enable/disable logging unknown scripts.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
web-filter-vbs-log	Enable/disable logging VBS scripts.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
web-ftgd-err-log	Enable/disable logging rating errors.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
web-ftgd-quota-usage	Enable/disable logging daily quota usage.	option	-	enable

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
web-invalid-domain-log	Enable/disable logging invalid domain names.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
web-url-log	Enable/disable logging URL filtering.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
wisp	Enable/disable web proxy WISP.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable web proxy WISP.		
	<i>disable</i>	Disable web proxy WISP.		
wisp-algorithm	WISP server selection algorithm.	option	-	auto-learning
	<b>Option</b>	<b>Description</b>		
	<i>primary-secondary</i>	Select the first healthy server in order.		
	<i>round-robin</i>	Select the next healthy server.		
	<i>auto-learning</i>	Select the lightest loading healthy server.		
wisp-servers <name>	WISP servers. Server name.	string	Maximum length: 79	

## config antiphish

Parameter	Description	Type	Size	Default
status	Toggle AntiPhishing functionality.	option	-	disable

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable AntiPhishing functionality.</td></tr><tr><td><i>disable</i></td><td>Disable AntiPhishing functionality.</td></tr></table>		Option	Description	<i>enable</i>	Enable AntiPhishing functionality.	<i>disable</i>	Disable AntiPhishing functionality.				
	Option	Description										
	<i>enable</i>	Enable AntiPhishing functionality.										
<i>disable</i>	Disable AntiPhishing functionality.											
default-action	Action to be taken when there is no matching rule.	option	-	exempt								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>exempt</i></td><td>Exempt requests from matching.</td></tr><tr><td><i>log</i></td><td>Log all matched requests.</td></tr><tr><td><i>block</i></td><td>Block all matched requests.</td></tr></table>		Option	Description	<i>exempt</i>	Exempt requests from matching.	<i>log</i>	Log all matched requests.	<i>block</i>	Block all matched requests.		
	Option	Description										
	<i>exempt</i>	Exempt requests from matching.										
	<i>log</i>	Log all matched requests.										
<i>block</i>	Block all matched requests.											
check-uri	Enable/disable checking of GET URI parameters for known credentials.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable checking of GET URI for username and password fields.</td></tr><tr><td><i>disable</i></td><td>Disable checking of GET URI for username and password fields.</td></tr></table>		Option	Description	<i>enable</i>	Enable checking of GET URI for username and password fields.	<i>disable</i>	Disable checking of GET URI for username and password fields.				
	Option	Description										
	<i>enable</i>	Enable checking of GET URI for username and password fields.										
<i>disable</i>	Disable checking of GET URI for username and password fields.											
check-basic-auth	Enable/disable checking of HTTP Basic Auth field for known credentials.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable checking of HTTP Basic Auth field for known credentials.</td></tr><tr><td><i>disable</i></td><td>Disable checking of HTTP Basic Auth field for known credentials.</td></tr></table>		Option	Description	<i>enable</i>	Enable checking of HTTP Basic Auth field for known credentials.	<i>disable</i>	Disable checking of HTTP Basic Auth field for known credentials.				
	Option	Description										
	<i>enable</i>	Enable checking of HTTP Basic Auth field for known credentials.										
<i>disable</i>	Disable checking of HTTP Basic Auth field for known credentials.											
check-username-only	Enable/disable username only matching of credentials. Action will be taken for valid usernames regardless of password validity.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable username only credential matches.</td></tr><tr><td><i>disable</i></td><td>Disable username only credential matches.</td></tr></table>		Option	Description	<i>enable</i>	Enable username only credential matches.	<i>disable</i>	Disable username only credential matches.				
	Option	Description										
	<i>enable</i>	Enable username only credential matches.										
<i>disable</i>	Disable username only credential matches.											
max-body-len	Maximum size of a POST body to check for credentials.	integer	Minimum value: 0 Maximum value: 4294967295	65536								
authentication	Authentication methods.	option	-	domain-controller								



Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>domain-controller</i></td><td>Domain Controller to verify user credential.</td></tr><tr><td><i>ldap</i></td><td>LDAP to verify user credential.</td></tr></table>				Option	Description	<i>domain-controller</i>	Domain Controller to verify user credential.	<i>ldap</i>	LDAP to verify user credential.
	Option	Description								
	<i>domain-controller</i>	Domain Controller to verify user credential.								
<i>ldap</i>	LDAP to verify user credential.									
domain-controller	Domain for which to verify received credentials against.	string	Maximum length: 63							
ldap	LDAP server for which to verify received credentials against.	string	Maximum length: 63							

### config inspection-entries

Parameter	Description	Type	Size	Default								
name	Inspection target name.	string	Maximum length: 63									
fortiguard-category	FortiGuard category to match.	user	Not Specified	0								
action	Action to be taken upon an AntiPhishing match.	option	-	exempt								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>exempt</i></td><td>Exempt requests from matching.</td></tr><tr><td><i>log</i></td><td>Log all matched requests.</td></tr><tr><td><i>block</i></td><td>Block all matched requests.</td></tr></table>				Option	Description	<i>exempt</i>	Exempt requests from matching.	<i>log</i>	Log all matched requests.	<i>block</i>	Block all matched requests.
Option	Description											
<i>exempt</i>	Exempt requests from matching.											
<i>log</i>	Log all matched requests.											
<i>block</i>	Block all matched requests.											

### config custom-patterns

Parameter	Description	Type	Size	Default
pattern	Target pattern.	string	Maximum length: 255	
category	Category that the pattern matches.	option	-	username
	Option	Description		
	username	Pattern matches username fields.		
	password	Pattern matches password fields.		
type	Pattern will be treated either as a regex pattern or literal string.	option	-	regex

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>regex</i>	Pattern will be treated as a regex pattern.		
	<i>literal</i>	Pattern will be treated as a literal string.		

## config ftgd-wf

Parameter	Description	Type	Size	Default
options	Options for FortiGuard Web Filter.	option	-	ftgd-disable
	<b>Option</b>	<b>Description</b>		
	<i>error-allow</i>	Allow web pages with a rating error to pass through.		
	<i>rate-server-ip</i>	Rate the server IP in addition to the domain name.		
	<i>connect-request-bypass</i>	Bypass connection which has CONNECT request.		
	<i>ftgd-disable</i>	Disable FortiGuard scanning.		
exempt-quota	Do not stop quota for these categories.	user	Not Specified	17
ovrd	Allow web filter profile overrides.	user	Not Specified	
max-quota-timeout	Maximum FortiGuard quota used by single page view in seconds (excludes streams).	integer	Minimum value: 1 Maximum value: 86400	300
rate-javascript-urls	Enable/disable rating JavaScript by URL.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable rating JavaScript by URL.		
	<i>enable</i>	Enable rating JavaScript by URL.		
rate-css-urls	Enable/disable rating CSS by URL.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable rating CSS by URL.		
	<i>enable</i>	Enable rating CSS by URL.		
rate-crl-urls	Enable/disable rating CRL by URL.	option	-	enable

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable rating CRL by URL.		
	<i>enable</i>	Enable rating CRL by URL.		

## config filters

Parameter	Description	Type	Size	Default
id	ID number.	integer	Minimum value: 0 Maximum value: 255	0
category	Categories and groups the filter examines.	integer	Minimum value: 0 Maximum value: 255	0
action	Action to take for matches.	option	-	monitor
	<b>Option</b>	<b>Description</b>		
	<i>block</i>	Block access.		
	<i>authenticate</i>	Authenticate user before allowing access.		
	<i>monitor</i>	Allow access while logging the action.		
	<i>warning</i>	Allow access after warning the user.		
warn-duration	Duration of warnings.	user	Not Specified	5m
auth-usr-grp <name>	Groups with permission to authenticate. User group name.	string	Maximum length: 79	
log	Enable/disable logging.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
override-replacemsg	Override replacement message.	string	Maximum length: 28	
warning-prompt	Warning prompts in each category or each domain.	option	-	per-category

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>per-domain</i>	Per-domain warnings.		
	<i>per-category</i>	Per-category warnings.		
warning-duration-type	Re-display warning after closing browser or after a timeout.	option	-	timeout
	<b>Option</b>	<b>Description</b>		
	<i>session</i>	After session ends.		
	<i>timeout</i>	After timeout occurs.		

### config quota

Parameter	Description	Type	Size	Default
id	ID number.	integer	Minimum value: 0 Maximum value: 4294967295	0
category	FortiGuard categories to apply quota to (category action must be set to monitor).	user	Not Specified	
type	Quota type.	option	-	time
	<b>Option</b>	<b>Description</b>		
	<i>time</i>	Use a time-based quota.		
	<i>traffic</i>	Use a traffic-based quota.		
unit	Traffic quota unit of measurement.	option	-	MB
	<b>Option</b>	<b>Description</b>		
	<i>B</i>	Quota in bytes.		
	<i>KB</i>	Quota in kilobytes.		
	<i>MB</i>	Quota in megabytes.		
	<i>GB</i>	Quota in gigabytes.		

Parameter	Description	Type	Size	Default
value	Traffic quota value.	integer	Minimum value: 1 Maximum value: 4294967295	1024
duration	Duration of quota.	user	Not Specified	5m
override-replacemsg	Override replacement message.	string	Maximum length: 28	

### config override

Parameter	Description	Type	Size	Default												
ovrd-cookie	Allow/deny browser-based (cookie) overrides.	option	-	deny												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow browser-based (cookie) override.</td></tr><tr><td><i>deny</i></td><td>Deny browser-based (cookie) override.</td></tr></table>	Option	Description	<i>allow</i>	Allow browser-based (cookie) override.	<i>deny</i>	Deny browser-based (cookie) override.									
Option	Description															
<i>allow</i>	Allow browser-based (cookie) override.															
<i>deny</i>	Deny browser-based (cookie) override.															
ovrd-scope	Override scope.	option	-	user												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>user</i></td><td>Override for the user.</td></tr><tr><td><i>user-group</i></td><td>Override for the user's group.</td></tr><tr><td><i>ip</i></td><td>Override for the initiating IP.</td></tr><tr><td><i>browser</i></td><td>Create browser-based (cookie) override.</td></tr><tr><td><i>ask</i></td><td>Prompt for scope when initiating an override.</td></tr></table>	Option	Description	<i>user</i>	Override for the user.	<i>user-group</i>	Override for the user's group.	<i>ip</i>	Override for the initiating IP.	<i>browser</i>	Create browser-based (cookie) override.	<i>ask</i>	Prompt for scope when initiating an override.			
Option	Description															
<i>user</i>	Override for the user.															
<i>user-group</i>	Override for the user's group.															
<i>ip</i>	Override for the initiating IP.															
<i>browser</i>	Create browser-based (cookie) override.															
<i>ask</i>	Prompt for scope when initiating an override.															
profile-type	Override profile type.	option	-	list												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>list</i></td><td>Profile chosen from list.</td></tr><tr><td><i>radius</i></td><td>Profile determined by RADIUS server.</td></tr></table>	Option	Description	<i>list</i>	Profile chosen from list.	<i>radius</i>	Profile determined by RADIUS server.									
Option	Description															
<i>list</i>	Profile chosen from list.															
<i>radius</i>	Profile determined by RADIUS server.															
ovrd-dur-mode	Override duration mode.	option	-	constant												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>constant</i></td><td>Constant mode.</td></tr><tr><td><i>ask</i></td><td>Prompt for duration when initiating an override.</td></tr></table>	Option	Description	<i>constant</i>	Constant mode.	<i>ask</i>	Prompt for duration when initiating an override.									
Option	Description															
<i>constant</i>	Constant mode.															
<i>ask</i>	Prompt for duration when initiating an override.															

Parameter	Description	Type	Size	Default
ovrd-dur	Override duration.	user	Not Specified	15m
profile-attribute	Profile attribute to retrieve from the RADIUS server.	option	-	Login-LAT-Service
	Option	Description		
	<i>User-Name</i>	Use this attribute.		
	<i>NAS-IP-Address</i>	Use this attribute.		
	<i>Framed-IP-Address</i>	Use this attribute.		
	<i>Framed-IP-Netmask</i>	Use this attribute.		
	<i>Filter-Id</i>	Use this attribute.		
	<i>Login-IP-Host</i>	Use this attribute.		
	<i>Reply-Message</i>	Use this attribute.		
	<i>Callback-Number</i>	Use this attribute.		
	<i>Callback-Id</i>	Use this attribute.		
	<i>Framed-Route</i>	Use this attribute.		
	<i>Framed-IPX-Network</i>	Use this attribute.		
	<i>Class</i>	Use this attribute.		
	<i>Called-Station-Id</i>	Use this attribute.		
	<i>Calling-Station-Id</i>	Use this attribute.		
	<i>NAS-Identifier</i>	Use this attribute.		
	<i>Proxy-State</i>	Use this attribute.		
	<i>Login-LAT-Service</i>	Use this attribute.		
	<i>Login-LAT-Node</i>	Use this attribute.		
	<i>Login-LAT-Group</i>	Use this attribute.		
	<i>Framed-AppleTalk-Zone</i>	Use this attribute.		
	<i>Acct-Session-Id</i>	Use this attribute.		

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>Acct-Multi-Session-Id</i>	Use this attribute.		
ovrd-user-group <name>	User groups with permission to use the override. User group name.	string	Maximum length: 79	
profile <name>	Web filter profile with permission to create overrides. Web profile.	string	Maximum length: 79	

### config url-extraction

Parameter	Description	Type	Size	Default
status	Enable URL Extraction	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
server-fqdn	URL extraction server FQDN (fully qualified domain name)	string	Maximum length: 255	
redirect-header	HTTP header name to use for client redirect on blocked requests	string	Maximum length: 35	x-redirect
redirect-url	HTTP header value to use for client redirect on blocked requests	string	Maximum length: 255	
redirect-no-content	Enable / Disable empty message-body entity in HTTP response	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

## config web

Parameter	Description	Type	Size	Default												
bword-threshold	Banned word score threshold.	integer	Minimum value: 0 Maximum value: 2147483647	10												
bword-table	Banned word table ID.	integer	Minimum value: 0 Maximum value: 4294967295	0												
urlfilter-table	URL filter table ID.	integer	Minimum value: 0 Maximum value: 4294967295	0												
content-header-list	Content header list.	integer	Minimum value: 0 Maximum value: 4294967295	0												
blocklist	Enable/disable automatic addition of URLs detected by FortiSandbox to blocklist.	option	-	disable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable setting.</td></tr><tr><td>disable</td><td>Disable setting.</td></tr></table>				Option	Description	enable	Enable setting.	disable	Disable setting.						
Option	Description															
enable	Enable setting.															
disable	Disable setting.															
allowlist	FortiGuard allowlist settings.	option	-													
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>exempt-av</td><td>Exempt antivirus.</td></tr><tr><td>exempt-webcontent</td><td>Exempt web content.</td></tr><tr><td>exempt-activex-java-cookie</td><td>Exempt ActiveX-JAVA-Cookie.</td></tr><tr><td>exempt-dlp</td><td>Exempt DLP.</td></tr><tr><td>exempt-rangeblock</td><td>Exempt RangeBlock.</td></tr></table>				Option	Description	exempt-av	Exempt antivirus.	exempt-webcontent	Exempt web content.	exempt-activex-java-cookie	Exempt ActiveX-JAVA-Cookie.	exempt-dlp	Exempt DLP.	exempt-rangeblock	Exempt RangeBlock.
Option	Description															
exempt-av	Exempt antivirus.															
exempt-webcontent	Exempt web content.															
exempt-activex-java-cookie	Exempt ActiveX-JAVA-Cookie.															
exempt-dlp	Exempt DLP.															
exempt-rangeblock	Exempt RangeBlock.															



Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>extended-log-others</i>	Support extended log.		
safe-search	Safe search type.	option	-	
	<b>Option</b>	<b>Description</b>		
	<i>url</i>	Insert safe search string into URL.		
	<i>header</i>	Insert safe search header.		
youtube-restrict	YouTube EDU filter level.	option	-	none
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	Full access for YouTube.		
	<i>strict</i>	Strict access for YouTube.		
	<i>moderate</i>	Moderate access for YouTube.		
vimeo-restrict	Set Vimeo-restrict ("7" = don't show mature content, "134" = don't show unrated and mature content). A value of cookie "content_rating".	string	Maximum length: 63	
log-search	Enable/disable logging all search phrases.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
keyword-match <pattern>	Search keywords to log when match is found. Pattern/keyword to search for.	string	Maximum length: 79	**

\*\* Values may differ between models.

## config webfilter search-engine

Configure web filter search engines.

```
config webfilter search-engine
  Description: Configure web filter search engines.
  edit <name>
    set charset [utf-8|gb2312]
    set hostname {string}
    set query {string}
    set safesearch [disable|url|...]
```

```

        set safesearch-str {string}
        set url {string}
    next
end

```

## config webfilter search-engine

Parameter	Description	Type	Size	Default																		
charset	Search engine charset.	option	-	utf-8																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>utf-8</td><td>UTF-8 encoding.</td></tr><tr><td>gb2312</td><td>GB2312 encoding.</td></tr></table>				Option	Description	utf-8	UTF-8 encoding.	gb2312	GB2312 encoding.												
	Option	Description																				
	utf-8	UTF-8 encoding.																				
gb2312	GB2312 encoding.																					
hostname	Hostname (regular expression).	string	Maximum length: 127																			
name	Search engine name.	string	Maximum length: 35																			
query	Code used to prefix a query (must end with an equals character).	string	Maximum length: 15																			
safesearch	Safe search method. You can disable safe search, add the safe search string to URLs, or insert a safe search header.	option	-	disable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Site does not support safe search.</td></tr><tr><td>url</td><td>Safe search selected with a parameter in the URL.</td></tr><tr><td>header</td><td>Safe search selected by search header (i.e. youtube.edu).</td></tr><tr><td>translate</td><td>Perform URL FortiGuard check on HTTP requests parameter.</td></tr><tr><td>yt-pattern</td><td>Pattern to match YouTube channel ID.</td></tr><tr><td>yt-scan</td><td>Perform IPS scan.</td></tr><tr><td>yt-video</td><td>Pattern to match YouTube video name.</td></tr><tr><td>yt-channel</td><td>Pattern to match YouTube channel name.</td></tr></table>				Option	Description	disable	Site does not support safe search.	url	Safe search selected with a parameter in the URL.	header	Safe search selected by search header (i.e. youtube.edu).	translate	Perform URL FortiGuard check on HTTP requests parameter.	yt-pattern	Pattern to match YouTube channel ID.	yt-scan	Perform IPS scan.	yt-video	Pattern to match YouTube video name.	yt-channel	Pattern to match YouTube channel name.
	Option	Description																				
	disable	Site does not support safe search.																				
	url	Safe search selected with a parameter in the URL.																				
	header	Safe search selected by search header (i.e. youtube.edu).																				
	translate	Perform URL FortiGuard check on HTTP requests parameter.																				
	yt-pattern	Pattern to match YouTube channel ID.																				
	yt-scan	Perform IPS scan.																				
yt-video	Pattern to match YouTube video name.																					
yt-channel	Pattern to match YouTube channel name.																					
safesearch-str	Safe search parameter used in the URL.	string	Maximum length: 79																			
url	URL (regular expression).	string	Maximum length: 127																			

## config webfilter urlfilter

Configure URL filter lists.

```
config webfilter urlfilter
  Description: Configure URL filter lists.
  edit <id>
    set comment {var-string}
    config entries
      Description: URL filter entries.
      edit <id>
        set url {string}
        set type [simple|regex|...]
        set action [exempt|block|...]
        set antiphish-action [block|log]
        set status [enable|disable]
        set exempt {option1}, {option2}, ...
        set web-proxy-profile {string}
        set referrer-host {string}
        set dns-address-family [ipv4|ipv6|...]
      next
    end
    set ip-addr-block [enable|disable]
    set name {string}
    set one-arm-ips-urlfilter [enable|disable]
  next
end
```

## config webfilter urlfilter

Parameter	Description	Type	Size	Default						
comment	Optional comments.	var-string	Maximum length: 255							
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0						
ip-addr-block	Enable/disable blocking URLs when the hostname appears as an IP address.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable blocking URLs when the hostname appears as an IP address.</td></tr><tr><td><i>disable</i></td><td>Disable blocking URLs when the hostname appears as an IP address.</td></tr></table>				Option	Description	<i>enable</i>	Enable blocking URLs when the hostname appears as an IP address.	<i>disable</i>	Disable blocking URLs when the hostname appears as an IP address.
Option	Description									
<i>enable</i>	Enable blocking URLs when the hostname appears as an IP address.									
<i>disable</i>	Disable blocking URLs when the hostname appears as an IP address.									
name	Name of URL filter list.	string	Maximum length: 63							

Parameter	Description	Type	Size	Default
one-arm-ips-urlfilter	Enable/disable DNS resolver for one-arm IPS URL filter operation.	option	-	disable
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Enable DNS resolver for one-arm IPS URL filter operation.		
	<i>disable</i>	Disable DNS resolver for one-arm IPS URL filter operation.		

## config entries

Parameter	Description	Type	Size	Default
id	Id.	integer	Minimum value: 0 Maximum value: 4294967295	0
url	URL to be filtered.	string	Maximum length: 511	
type	Filter type (simple, regex, or wildcard).	option	-	simple
	<b>Option</b> <b>Description</b>			
	<i>simple</i>	Simple URL string.		
	<i>regex</i>	Regular expression URL string.		
	<i>wildcard</i>	Wildcard URL string.		
action	Action to take for URL filter matches.	option	-	exempt
	<b>Option</b> <b>Description</b>			
	<i>exempt</i>	Exempt matches.		
	<i>block</i>	Block matches.		
	<i>allow</i>	Allow matches (no log).		
	<i>monitor</i>	Allow matches (with log).		
antiphish-action	Action to take for AntiPhishing matches.	option	-	block
	<b>Option</b> <b>Description</b>			
	<i>block</i>	Block matches.		
	<i>log</i>	Allow matches with log.		

Parameter	Description	Type	Size	Default																				
status	Enable/disable this URL filter.	option	-	enable																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable this URL filter.</td></tr><tr><td><i>disable</i></td><td>Disable this URL filter.</td></tr></table>				Option	Description	<i>enable</i>	Enable this URL filter.	<i>disable</i>	Disable this URL filter.														
	Option	Description																						
	<i>enable</i>	Enable this URL filter.																						
<i>disable</i>	Disable this URL filter.																							
exempt	If action is set to exempt, select the security profile operations that exempt URLs skip. Separate multiple options with a space.	option	-	av web-content activex-java-cookie dlp fortiguard range-block antiphish all																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>av</i></td><td>AntiVirus scanning.</td></tr><tr><td><i>web-content</i></td><td>Web filter content matching.</td></tr><tr><td><i>activex-java-cookie</i></td><td>ActiveX, Java, and cookie filtering.</td></tr><tr><td><i>dlp</i></td><td>DLP scanning.</td></tr><tr><td><i>fortiguard</i></td><td>FortiGuard web filtering.</td></tr><tr><td><i>range-block</i></td><td>Range block feature.</td></tr><tr><td><i>pass</i></td><td>Pass single connection from all.</td></tr><tr><td><i>antiphish</i></td><td>AntiPhish credential checking.</td></tr><tr><td><i>all</i></td><td>Exempt from all security profiles.</td></tr></table>				Option	Description	<i>av</i>	AntiVirus scanning.	<i>web-content</i>	Web filter content matching.	<i>activex-java-cookie</i>	ActiveX, Java, and cookie filtering.	<i>dlp</i>	DLP scanning.	<i>fortiguard</i>	FortiGuard web filtering.	<i>range-block</i>	Range block feature.	<i>pass</i>	Pass single connection from all.	<i>antiphish</i>	AntiPhish credential checking.	<i>all</i>	Exempt from all security profiles.
	Option	Description																						
	<i>av</i>	AntiVirus scanning.																						
	<i>web-content</i>	Web filter content matching.																						
	<i>activex-java-cookie</i>	ActiveX, Java, and cookie filtering.																						
	<i>dlp</i>	DLP scanning.																						
	<i>fortiguard</i>	FortiGuard web filtering.																						
	<i>range-block</i>	Range block feature.																						
	<i>pass</i>	Pass single connection from all.																						
<i>antiphish</i>	AntiPhish credential checking.																							
<i>all</i>	Exempt from all security profiles.																							
web-proxy-profile	Web proxy profile.	string	Maximum length: 63																					
referrer-host	Referrer host name.	string	Maximum length: 255																					
dns-address-family	Resolve IPv4 address, IPv6 address, or both from DNS server.	option	-	ipv4																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ipv4</i></td><td>Resolve IPv4 address from DNS server.</td></tr><tr><td><i>ipv6</i></td><td>Resolve IPv6 address from DNS server.</td></tr><tr><td><i>both</i></td><td>Resolve both IPv4 and IPv6 addresses from DNS server.</td></tr></table>				Option	Description	<i>ipv4</i>	Resolve IPv4 address from DNS server.	<i>ipv6</i>	Resolve IPv6 address from DNS server.	<i>both</i>	Resolve both IPv4 and IPv6 addresses from DNS server.												
	Option	Description																						
	<i>ipv4</i>	Resolve IPv4 address from DNS server.																						
	<i>ipv6</i>	Resolve IPv6 address from DNS server.																						
<i>both</i>	Resolve both IPv4 and IPv6 addresses from DNS server.																							

## wireless-controller

This section includes syntax for the following commands:

- [config wireless-controller access-control-list on page 1907](#)
- [config wireless-controller address on page 1909](#)
- [config wireless-controller addrgrp on page 1910](#)
- [config wireless-controller ap-status on page 1911](#)
- [config wireless-controller apcfg-profile on page 1911](#)
- [config wireless-controller arrp-profile on page 1913](#)
- [config wireless-controller ble-profile on page 1916](#)
- [config wireless-controller bonjour-profile on page 1918](#)
- [config wireless-controller global on page 1920](#)
- [config wireless-controller hotspot20 anqp-3gpp-cellular on page 1923](#)
- [config wireless-controller hotspot20 anqp-ip-address-type on page 1924](#)
- [config wireless-controller hotspot20 anqp-nai-realm on page 1925](#)
- [config wireless-controller hotspot20 anqp-network-auth-type on page 1929](#)
- [config wireless-controller hotspot20 anqp-roaming-consortium on page 1929](#)
- [config wireless-controller hotspot20 anqp-venue-name on page 1930](#)
- [config wireless-controller hotspot20 anqp-venue-url on page 1931](#)
- [config wireless-controller hotspot20 h2qp-advice-of-charge on page 1932](#)
- [config wireless-controller hotspot20 h2qp-conn-capability on page 1933](#)
- [config wireless-controller hotspot20 h2qp-operator-name on page 1936](#)
- [config wireless-controller hotspot20 h2qp-osu-provider-nai on page 1937](#)
- [config wireless-controller hotspot20 h2qp-osu-provider on page 1938](#)
- [config wireless-controller hotspot20 h2qp-terms-and-conditions on page 1939](#)
- [config wireless-controller hotspot20 h2qp-wan-metric on page 1940](#)
- [config wireless-controller hotspot20 hs-profile on page 1941](#)
- [config wireless-controller hotspot20 icon on page 1949](#)
- [config wireless-controller hotspot20 qos-map on page 1950](#)
- [config wireless-controller inter-controller on page 1952](#)
- [config wireless-controller log on page 1954](#)
- [config wireless-controller mpsk-profile on page 1958](#)
- [config wireless-controller nac-profile on page 1960](#)
- [config wireless-controller qos-profile on page 1961](#)
- [config wireless-controller region on page 1964](#)
- [config wireless-controller setting on page 1965](#)
- [config wireless-controller snmp on page 1974](#)
- [config wireless-controller ssid-policy on page 1978](#)
- [config wireless-controller syslog-profile on page 1979](#)
- [config wireless-controller timers on page 1980](#)

- [config wireless-controller vap-group on page 1982](#)
- [config wireless-controller vap on page 1983](#)
- [config wireless-controller wag-profile on page 2015](#)
- [config wireless-controller wids-profile on page 2017](#)
- [config wireless-controller wtp-group on page 2024](#)
- [config wireless-controller wtp-profile on page 2027](#)
- [config wireless-controller wtp on page 2099](#)

## config wireless-controller access-control-list

Configure WiFi bridge access control list.

```
config wireless-controller access-control-list
  Description: Configure WiFi bridge access control list.
  edit <name>
    set comment {string}
    config layer3-ipv4-rules
      Description: AP ACL layer3 ipv4 rule list.
      edit <rule-id>
        set comment {string}
        set srcaddr {user}
        set srcport {integer}
        set dstaddr {user}
        set dstport {integer}
        set protocol {integer}
        set action [allow|deny]
      next
    end
    config layer3-ipv6-rules
      Description: AP ACL layer3 ipv6 rule list.
      edit <rule-id>
        set comment {string}
        set srcaddr {user}
        set srcport {integer}
        set dstaddr {user}
        set dstport {integer}
        set protocol {integer}
        set action [allow|deny]
      next
    end
  next
end
```

## config wireless-controller access-control-list

Parameter	Description	Type	Size	Default
comment	Description.	string	Maximum length: 63	
name	AP access control list name.	string	Maximum length: 35	

## config layer3-ipv4-rules

Parameter	Description	Type	Size	Default
rule-id	Rule ID.	integer	Minimum value: 1 Maximum value: 65535	0
comment	Description.	string	Maximum length: 63	
srcaddr	Source IP address.	user	Not Specified	
srcport	Source port.	integer	Minimum value: 0 Maximum value: 65535	0
dstaddr	Destination IP address.	user	Not Specified	
dstport	Destination port.	integer	Minimum value: 0 Maximum value: 65535	0
protocol	Protocol type as defined by IANA.	integer	Minimum value: 0 Maximum value: 255	255
action	Policy action (allow   deny).	option	-	
	Option	Description		
	allow	Allows traffic matching the policy.		
	deny	Blocks traffic matching the policy.		

## config layer3-ipv6-rules

Parameter	Description	Type	Size	Default
rule-id	Rule ID.	integer	Minimum value: 1 Maximum value: 65535	0



Parameter	Description	Type	Size	Default						
comment	Description.	string	Maximum length: 63							
srcaddr	Source IPv6 address (any   local-LAN   IPv6 address [/prefix length]), default = any.	user	Not Specified							
srcport	Source port.	integer	Minimum value: 0 Maximum value: 65535	0						
dstaddr	Destination IPv6 address (any   local-LAN   IPv6 address [/prefix length]), default = any.	user	Not Specified							
dstport	Destination port.	integer	Minimum value: 0 Maximum value: 65535	0						
protocol	Protocol type as defined by IANA.	integer	Minimum value: 0 Maximum value: 255	255						
action	Policy action (allow   deny).	option	-							
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allows traffic matching the policy.</td></tr><tr><td><i>deny</i></td><td>Blocks traffic matching the policy.</td></tr></table>				Option	Description	<i>allow</i>	Allows traffic matching the policy.	<i>deny</i>	Blocks traffic matching the policy.
Option	Description									
<i>allow</i>	Allows traffic matching the policy.									
<i>deny</i>	Blocks traffic matching the policy.									

## config wireless-controller address

Configure the client with its MAC address.

```

config wireless-controller address
    Description: Configure the client with its MAC address.
    edit <id>
        set mac {mac-address}
        set policy [allow|deny]
    next
end

```

## config wireless-controller address

Parameter	Description	Type	Size	Default
id	ID.	string	Maximum length: 35	
mac	MAC address.	mac-address	Not Specified	00:00:00:00:00:00
policy	Allow or block the client with this MAC address.	option	-	deny
	Option	Description		
	<i>allow</i>	Allow the client with this MAC address.		
	<i>deny</i>	Block the client with this MAC address.		

## config wireless-controller addrgrp

Configure the MAC address group.

```
config wireless-controller addrgrp
  Description: Configure the MAC address group.
  edit <id>
    set addresses <id1>, <id2>, ...
    set default-policy [allow|deny]
  next
end
```

## config wireless-controller addrgrp

Parameter	Description	Type	Size	Default						
addresses <id>	Manually selected group of addresses. Address ID.	string	Maximum length: 35							
default-policy	Allow or block the clients with MAC addresses that are not in the group.	option	-	allow						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>allow</td><td>Allow the clients with MAC addresses that are not in the group.</td></tr><tr><td>deny</td><td>Block the clients with MAC addresses that are not in the group.</td></tr></table>				Option	Description	allow	Allow the clients with MAC addresses that are not in the group.	deny	Block the clients with MAC addresses that are not in the group.
	Option	Description								
	allow	Allow the clients with MAC addresses that are not in the group.								
deny	Block the clients with MAC addresses that are not in the group.									
id	ID.	string	Maximum length: 35							

## config wireless-controller ap-status

Configure access point status (rogue | accepted | suppressed).

```
config wireless-controller ap-status
  Description: Configure access point status (rogue | accepted | suppressed).
  edit <id>
    set bssid {mac-address}
    set ssid {string}
    set status [rogue|accepted|...]
  next
end
```

## config wireless-controller ap-status

Parameter	Description	Type	Size	Default
bssid	Access Point's (AP's) BSSID.	mac-address	Not Specified	00:00:00:00:00:00
id	AP ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
ssid	Access Point's (AP's) SSID.	string	Maximum length: 32	
status	Access Point's (AP's) status: rogue, accepted, or suppressed.	option	-	rogue
		Option	Description	
		<i>rogue</i>	Rogue AP.	
		<i>accepted</i>	Accepted AP.	
		<i>suppressed</i>	Suppressed AP.	

## config wireless-controller apcfg-profile

Configure AP local configuration profiles.

```
config wireless-controller apcfg-profile
  Description: Configure AP local configuration profiles.
  edit <name>
    set ac-ip {ipv4-address}
    set ac-port {integer}
    set ac-timer {integer}
    set ac-type [default|specify|...]
    set ap-family [fap|fap-u|...]
    config command-list
```

```

        Description: AP local configuration command list.
        edit <id>
            set type [non-password|password]
            set name {string}
            set value {string}
            set passwd-value {password}
        next
    end
    set comment {var-string}
next
end

```

## config wireless-controller apcfg-profile

Parameter	Description	Type	Size	Default
ac-ip	IP address of the validation controller that AP must be able to join after applying AP local configuration.	ipv4-address	Not Specified	0.0.0.0
ac-port	Port of the validation controller that AP must be able to join after applying AP local configuration.	integer	Minimum value: 1024 Maximum value: 49150	0
ac-timer	Maximum waiting time for the AP to join the validation controller after applying AP local configuration.	integer	Minimum value: 3 Maximum value: 30	10
ac-type	Validation controller type.	option	-	default
	<b>Option</b>		<b>Description</b>	
	<i>default</i>	This controller is the one and only controller that the AP could join after applying AP local configuration.		
	<i>specify</i>	Specified controller is the one and only controller that the AP could join after applying AP local configuration.		
	<i>apcfg</i>	Any controller defined by AP local configuration after applying AP local configuration.		
ap-family	FortiAP family type.	option	-	fap
	<b>Option</b>		<b>Description</b>	
	<i>fap</i>	FortiAP Family.		
	<i>fap-u</i>	FortiAP-U Family.		
	<i>fap-c</i>	FortiAP-C Family.		

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 255	
name	AP local configuration profile name.	string	Maximum length: 35	

## config command-list

Parameter	Description	Type	Size	Default						
id	Command ID.	integer	Minimum value: 1 Maximum value: 255	0						
type	The command type.	option	-	non-password						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>non-password</i></td><td>Non-password command.</td></tr><tr><td><i>password</i></td><td>Password command.</td></tr></table>				Option	Description	<i>non-password</i>	Non-password command.	<i>password</i>	Password command.
	Option	Description								
	<i>non-password</i>	Non-password command.								
<i>password</i>	Password command.									
name	AP local configuration command name.	string	Maximum length: 63							
value	AP local configuration command value.	string	Maximum length: 127							
passwd-value	AP local configuration command password value.	password	Not Specified							

## config wireless-controller arrp-profile

Configure WiFi Automatic Radio Resource Provisioning (ARRP) profiles.

```
config wireless-controller arrp-profile
  Description: Configure WiFi Automatic Radio Resource Provisioning (ARRP) profiles.
  edit <name>
    set comment {var-string}
    set darrp-optimize {integer}
    set darrp-optimize-schedules <name1>, <name2>, ...
    set include-dfs-channel [enable|disable]
    set include-weather-channel [enable|disable]
    set monitor-period {integer}
    set override-darrp-optimize [enable|disable]
    set selection-period {integer}
    set threshold-ap {integer}
    set threshold-channel-load {integer}
    set threshold-noise-floor {string}
    set threshold-rx-errors {integer}
```

```

        set threshold-spectral-rssi {string}
        set threshold-tx-retries {integer}
        set weight-channel-load {integer}
        set weight-dfs-channel {integer}
        set weight-managed-ap {integer}
        set weight-noise-floor {integer}
        set weight-rogue-ap {integer}
        set weight-spectral-rssi {integer}
        set weight-weather-channel {integer}
    next
end

```

## config wireless-controller arrp-profile

Parameter	Description	Type	Size	Default						
comment	Comment.	var-string	Maximum length: 255							
darrp-optimize	Time for running Dynamic Automatic Radio Resource Provisioning.	integer	Minimum value: 0 Maximum value: 86400	86400						
darrp-optimize-schedules <name>	Firewall schedules for DARRP running time. DARRP will run periodically based on darrp-optimize within the schedules. Separate multiple schedule names with a space. Schedule name.	string	Maximum length: 35							
include-dfs-channel	Enable/disable use of DFS channel in DARRP channel selection phase 1.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Include DFS channel in darrp channel selection phase 1.</td></tr><tr><td>disable</td><td>Exclude DFS channel in darrp channel selection phase 1.</td></tr></table>				Option	Description	enable	Include DFS channel in darrp channel selection phase 1.	disable	Exclude DFS channel in darrp channel selection phase 1.
Option	Description									
enable	Include DFS channel in darrp channel selection phase 1.									
disable	Exclude DFS channel in darrp channel selection phase 1.									
include-weather-channel	Enable/disable use of weather channel in DARRP channel selection phase 1.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Include weather channel in darrp channel selection phase 1.</td></tr><tr><td>disable</td><td>Exclude weather channel in darrp channel selection phase 1.</td></tr></table>				Option	Description	enable	Include weather channel in darrp channel selection phase 1.	disable	Exclude weather channel in darrp channel selection phase 1.
Option	Description									
enable	Include weather channel in darrp channel selection phase 1.									
disable	Exclude weather channel in darrp channel selection phase 1.									

Parameter	Description	Type	Size	Default
monitor-period	Period in seconds to measure average transmit retries and receive errors.	integer	Minimum value: 0 Maximum value: 65535	300
name	WiFi ARRP profile name.	string	Maximum length: 35	
override-darrp-optimize	Enable to override setting darrp-optimize and darrp-optimize-schedules.	option	-	disable
	Option	Description		
	enable	Override setting darrp-optimize and darrp-optimize-schedules.		
	disable	Use setting darrp-optimize and darrp-optimize-schedules.		
selection-period	Period in seconds to measure average channel load, noise floor, spectral RSSI.	integer	Minimum value: 0 Maximum value: 65535	3600
threshold-ap	Threshold to reject channel in DARRP channel selection phase 1 due to surrounding APs.	integer	Minimum value: 0 Maximum value: 500	250
threshold-channel-load	Threshold in percentage to reject channel in DARRP channel selection phase 1 due to channel load.	integer	Minimum value: 0 Maximum value: 100	60
threshold-noise-floor	Threshold in dBm to reject channel in DARRP channel selection phase 1 due to noise floor.	string	Maximum length: 7	-85
threshold-rx-errors	Threshold in percentage for receive errors to trigger channel reselection in DARRP monitor stage.	integer	Minimum value: 0 Maximum value: 100	50
threshold-spectral-rssi	Threshold in dBm to reject channel in DARRP channel selection phase 1 due to spectral RSSI.	string	Maximum length: 7	-65
threshold-tx-retries	Threshold in percentage for transmit retries to trigger channel reselection in DARRP monitor stage.	integer	Minimum value: 0 Maximum value: 1000	300

Parameter	Description	Type	Size	Default
weight-channel-load	Weight in DARRP channel score calculation for channel load.	integer	Minimum value: 0 Maximum value: 2000	20
weight-dfs-channel	Weight in DARRP channel score calculation for DFS channel.	integer	Minimum value: 0 Maximum value: 2000	500
weight-managed-ap	Weight in DARRP channel score calculation for managed APs.	integer	Minimum value: 0 Maximum value: 2000	50
weight-noise-floor	Weight in DARRP channel score calculation for noise floor.	integer	Minimum value: 0 Maximum value: 2000	40
weight-rogue-ap	Weight in DARRP channel score calculation for rogue APs.	integer	Minimum value: 0 Maximum value: 2000	10
weight-spectral-rssi	Weight in DARRP channel score calculation for spectral RSSI.	integer	Minimum value: 0 Maximum value: 2000	40
weight-weather-channel	Weight in DARRP channel score calculation for weather channel.	integer	Minimum value: 0 Maximum value: 2000	1000

## config wireless-controller ble-profile

Configure Bluetooth Low Energy profile.

```

config wireless-controller ble-profile
    Description: Configure Bluetooth Low Energy profile.
    edit <name>
        set advertising {option1}, {option2}, ...
        set beacon-interval {integer}
        set ble-scanning [enable|disable]
        set comment {string}
        set eddystone-instance {string}
        set eddystone-namespace {string}
        set eddystone-url {string}
        set ibeacon-uuid {string}
        set major-id {integer}

```



```

        set minor-id {integer}
        set txpower [0|1|...]
    next
end

```

## config wireless-controller ble-profile

Parameter	Description	Type	Size	Default
advertising	Advertising type.	option	-	
	<b>Option</b>	<b>Description</b>		
	<i>ibeacon</i>	iBeacon advertising.		
	<i>eddystone-uid</i>	Eddystone UID advertising.		
	<i>eddystone-url</i>	Eddystone URL advertising.		
beacon-interval	Beacon interval.	integer	Minimum value: 40 Maximum value: 3500	100
ble-scanning	Enable/disable Bluetooth Low Energy (BLE) scanning.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable BLE scanning.		
	<i>disable</i>	Disable BLE scanning.		
comment	Comment.	string	Maximum length: 63	
eddystone-instance	Eddystone instance ID.	string	Maximum length: 12	abcdef
eddystone-namespace	Eddystone namespace ID.	string	Maximum length: 20	0102030405
eddystone-url	Eddystone URL.	string	Maximum length: 127	http://www.fortinet.com
ibeacon-uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	string	Maximum length: 63	005ea414-cbd1-11e5-9956-625662870761
major-id	Major ID.	integer	Minimum value: 0 Maximum value: 65535	1000

Parameter	Description	Type	Size	Default
minor-id	Minor ID.	integer	Minimum value: 0 Maximum value: 65535	2000
name	Bluetooth Low Energy profile name.	string	Maximum length: 35	
txpower	Transmit power level.	option	-	0
	Option	Description		
	0	Transmit power level 0 (-21 dBm)		
	1	Transmit power level 1 (-18 dBm)		
	2	Transmit power level 2 (-15 dBm)		
	3	Transmit power level 3 (-12 dBm)		
	4	Transmit power level 4 (-9 dBm)		
	5	Transmit power level 5 (-6 dBm)		
	6	Transmit power level 6 (-3 dBm)		
	7	Transmit power level 7 (0 dBm)		
	8	Transmit power level 8 (1 dBm)		
	9	Transmit power level 9 (2 dBm)		
	10	Transmit power level 10 (3 dBm)		
	11	Transmit power level 11 (4 dBm)		
	12	Transmit power level 12 (5 dBm)		

## config wireless-controller bonjour-profile

Configure Bonjour profiles. Bonjour is Apple's zero configuration networking protocol. Bonjour profiles allow APs and FortiAPs to connect to networks using Bonjour.

```
config wireless-controller bonjour-profile
    Description: Configure Bonjour profiles. Bonjour is Apple's zero configuration
networking protocol. Bonjour profiles allow APs and FortiAPs to connect to networks using
Bonjour.
    edit <name>
        set comment {string}
        config policy-list
            Description: Bonjour policy list.
            edit <policy-id>
                set description {string}
                set from-vlan {string}
```

```

        set to-vlan {string}
        set services {option1}, {option2}, ...
    next
end
next
end

```

## config wireless-controller bonjour-profile

Parameter	Description	Type	Size	Default
comment	Comment.	string	Maximum length: 63	
name	Bonjour profile name.	string	Maximum length: 35	

## config policy-list

Parameter	Description	Type	Size	Default
policy-id	Policy ID.	integer	Minimum value: 1 Maximum value: 65535	0
description	Description.	string	Maximum length: 63	
from-vlan	VLAN ID from which the Bonjour service is advertised.	string	Maximum length: 63	0
to-vlan	VLAN ID to which the Bonjour service is made available.	string	Maximum length: 63	all
services	Bonjour services for the VLAN connecting to the Bonjour network.	option	-	all

Option	Description
<i>all</i>	All services.
<i>airplay</i>	AirPlay.
<i>afp</i>	AFP (Apple File Sharing).
<i>bit-torrent</i>	BitTorrent.
<i>ftp</i>	FTP.
<i>ichat</i>	iChat.
<i>itunes</i>	iTunes.

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>printers</i>	Printers.		
	<i>samba</i>	Samba.		
	<i>scanners</i>	Scanners.		
	<i>ssh</i>	SSH.		
	<i>chromecast</i>	ChromeCast.		

## config wireless-controller global

Configure wireless controller global settings.

```
config wireless-controller global
    Description: Configure wireless controller global settings.
    set ap-log-server [enable|disable]
    set ap-log-server-ip {ipv4-address}
    set ap-log-server-port {integer}
    set control-message-offload {option1}, {option2}, ...
    set data-ethernet-II [enable|disable]
    set dfs-lab-test [enable|disable]
    set discovery-mc-addr {ipv4-address-multicast}
    set fiapp-eth-type {integer}
    set image-download [enable|disable]
    set ipsec-base-ip {ipv4-address}
    set link-aggregation [enable|disable]
    set local-radio-vdom {string}
    set location {string}
    set max-clients {integer}
    set max-retransmit {integer}
    set mesh-eth-type {integer}
    set nac-interval {integer}
    set name {string}
    set rogue-scan-mac-adjacency {integer}
    set tunnel-mode [compatible|strict]
    set wtp-share [enable|disable]
end
```

## config wireless-controller global

Parameter	Description	Type	Size	Default
ap-log-server	Enable/disable configuring FortiGate to redirect wireless event log messages or FortiAPs to send UTM log messages to a syslog server.	option	-	disable

Parameter	Description	Type	Size	Default																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable AP log server.</td></tr><tr><td><i>disable</i></td><td>Disable AP log server.</td></tr></table>	Option	Description	<i>enable</i>	Enable AP log server.	<i>disable</i>	Disable AP log server.																	
	Option	Description																						
	<i>enable</i>	Enable AP log server.																						
<i>disable</i>	Disable AP log server.																							
ap-log-server-ip	IP address that FortiGate or FortiAPs send log messages to.	ipv4-address	Not Specified	0.0.0.0																				
ap-log-server-port	Port that FortiGate or FortiAPs send log messages to.	integer	Minimum value: 0 Maximum value: 65535	0																				
control-message-offload	Configure CAPWAP control message data channel offload.	option	-	ebp-frame aeroscout-tag ap-list sta-list sta-cap-list stats aeroscout-mu sta-health spectral-analysis																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ebp-frame</i></td><td>Ekahau blink protocol (EBP) frames.</td></tr><tr><td><i>aeroscout-tag</i></td><td>AeroScout tag.</td></tr><tr><td><i>ap-list</i></td><td>Rogue AP list.</td></tr><tr><td><i>sta-list</i></td><td>Rogue STA list.</td></tr><tr><td><i>sta-cap-list</i></td><td>STA capability list.</td></tr><tr><td><i>stats</i></td><td>WTP, radio, VAP, and STA statistics.</td></tr><tr><td><i>aeroscout-mu</i></td><td>AeroScout Mobile Unit (MU) report.</td></tr><tr><td><i>sta-health</i></td><td>STA health log.</td></tr><tr><td><i>spectral-analysis</i></td><td>Spectral analysis report.</td></tr></table>	Option	Description	<i>ebp-frame</i>	Ekahau blink protocol (EBP) frames.	<i>aeroscout-tag</i>	AeroScout tag.	<i>ap-list</i>	Rogue AP list.	<i>sta-list</i>	Rogue STA list.	<i>sta-cap-list</i>	STA capability list.	<i>stats</i>	WTP, radio, VAP, and STA statistics.	<i>aeroscout-mu</i>	AeroScout Mobile Unit (MU) report.	<i>sta-health</i>	STA health log.	<i>spectral-analysis</i>	Spectral analysis report.			
	Option	Description																						
	<i>ebp-frame</i>	Ekahau blink protocol (EBP) frames.																						
	<i>aeroscout-tag</i>	AeroScout tag.																						
	<i>ap-list</i>	Rogue AP list.																						
	<i>sta-list</i>	Rogue STA list.																						
	<i>sta-cap-list</i>	STA capability list.																						
	<i>stats</i>	WTP, radio, VAP, and STA statistics.																						
	<i>aeroscout-mu</i>	AeroScout Mobile Unit (MU) report.																						
<i>sta-health</i>	STA health log.																							
<i>spectral-analysis</i>	Spectral analysis report.																							
data-ethernet-II	Configure the wireless controller to use Ethernet II or 802.3 frames with 802.3 data tunnel mode.	option	-	enable																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Use Ethernet II frames with 802.3 data tunnel mode.</td></tr><tr><td><i>disable</i></td><td>Use 802.3 Ethernet frames with 802.3 data tunnel mode.</td></tr></table>	Option	Description	<i>enable</i>	Use Ethernet II frames with 802.3 data tunnel mode.	<i>disable</i>	Use 802.3 Ethernet frames with 802.3 data tunnel mode.																	
	Option	Description																						
	<i>enable</i>	Use Ethernet II frames with 802.3 data tunnel mode.																						
<i>disable</i>	Use 802.3 Ethernet frames with 802.3 data tunnel mode.																							

Parameter	Description	Type	Size	Default						
dfs-lab-test	Enable/disable DFS certificate lab test mode.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable DFS certificate lab test mode.</td></tr><tr><td><i>disable</i></td><td>Disable DFS certificate lab test mode.</td></tr></table>	Option	Description	<i>enable</i>	Enable DFS certificate lab test mode.	<i>disable</i>	Disable DFS certificate lab test mode.			
Option	Description									
<i>enable</i>	Enable DFS certificate lab test mode.									
<i>disable</i>	Disable DFS certificate lab test mode.									
discovery-mc-addr	Multicast IP address for AP discovery.	ipv4-address-multicast	Not Specified	224.0.1.140						
fiapp-eth-type	Ethernet type for Fortinet Inter-Access Point Protocol.	integer	Minimum value: 0 Maximum value: 65535	5252						
image-download	Enable/disable WTP image download at join time.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable WTP image download at join time.</td></tr><tr><td><i>disable</i></td><td>Disable WTP image download at join time.</td></tr></table>	Option	Description	<i>enable</i>	Enable WTP image download at join time.	<i>disable</i>	Disable WTP image download at join time.			
Option	Description									
<i>enable</i>	Enable WTP image download at join time.									
<i>disable</i>	Disable WTP image download at join time.									
ipsec-base-ip	Base IP address for IPsec VPN tunnels between the access points and the wireless controller.	ipv4-address	Not Specified	169.254.0.1						
link-aggregation	Enable/disable calculating the CAPWAP transmit hash to load balance sessions to link aggregation nodes.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable calculating the CAPWAP transmit hash.</td></tr><tr><td><i>disable</i></td><td>Disable calculating the CAPWAP transmit hash.</td></tr></table>	Option	Description	<i>enable</i>	Enable calculating the CAPWAP transmit hash.	<i>disable</i>	Disable calculating the CAPWAP transmit hash.			
Option	Description									
<i>enable</i>	Enable calculating the CAPWAP transmit hash.									
<i>disable</i>	Disable calculating the CAPWAP transmit hash.									
local-radio-vdom *	Assign local radio's virtual domain.	string	Maximum length: 31	root						
location	Description of the location of the wireless controller.	string	Maximum length: 35							
max-clients	Maximum number of clients that can connect simultaneously.	integer	Minimum value: 0 Maximum value: 4294967295	0						

Parameter	Description	Type	Size	Default						
max-retransmit	Maximum number of tunnel packet retransmissions.	integer	Minimum value: 0 Maximum value: 64	3						
mesh-eth-type	Mesh Ethernet identifier included in backhaul packets.	integer	Minimum value: 0 Maximum value: 65535	8755						
nac-interval	Interval in seconds between two WiFi network access control.	integer	Minimum value: 10 Maximum value: 600	120						
name	Name of the wireless controller.	string	Maximum length: 35							
rogue-scan-mac-adjacency	Maximum numerical difference between an AP's Ethernet and wireless MAC values to match for rogue detection.	integer	Minimum value: 0 Maximum value: 31	7						
tunnel-mode	Compatible/strict tunnel mode.	option	-	compatible						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>compatible</i></td><td>Allow for backward compatible ciphers(3DES+SHA1+Strong list).</td></tr><tr><td><i>strict</i></td><td>Follow system level strong-crypto ciphers.</td></tr></table>				Option	Description	<i>compatible</i>	Allow for backward compatible ciphers(3DES+SHA1+Strong list).	<i>strict</i>	Follow system level strong-crypto ciphers.
Option	Description									
<i>compatible</i>	Allow for backward compatible ciphers(3DES+SHA1+Strong list).									
<i>strict</i>	Follow system level strong-crypto ciphers.									
wtp-share	Enable/disable sharing of WTPs between VDOMs.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>WTP can be shared between all VDOMs.</td></tr><tr><td><i>disable</i></td><td>WTP can be used only in its own VDOM.</td></tr></table>				Option	Description	<i>enable</i>	WTP can be shared between all VDOMs.	<i>disable</i>	WTP can be used only in its own VDOM.
Option	Description									
<i>enable</i>	WTP can be shared between all VDOMs.									
<i>disable</i>	WTP can be used only in its own VDOM.									

\* This parameter may not exist in some models.

## config wireless-controller hotspot20 anqp-3gpp-cellular

Configure 3GPP public land mobile network (PLMN).

```
config wireless-controller hotspot20 anqp-3gpp-cellular
  Description: Configure 3GPP public land mobile network (PLMN).
  edit <name>
    config mcc-mnc-list
      Description: Mobile Country Code and Mobile Network Code configuration.
      edit <id>
```

```

        set mcc {string}
        set mnc {string}
    next
end
next
end

```

## config wireless-controller hotspot20 anqp-3gpp-cellular

Parameter	Description	Type	Size	Default
name	3GPP PLMN name.	string	Maximum length: 35	

## config mcc-mnc-list

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 1 Maximum value: 6	0
mcc	Mobile country code.	string	Maximum length: 3	
mnc	Mobile network code.	string	Maximum length: 3	

## config wireless-controller hotspot20 anqp-ip-address-type

Configure IP address type availability.

```

config wireless-controller hotspot20 anqp-ip-address-type
    Description: Configure IP address type availability.
    edit <name>
        set ipv4-address-type [not-available|public|...]
        set ipv6-address-type [not-available|available|...]
    next
end

```

## config wireless-controller hotspot20 anqp-ip-address-type

Parameter	Description	Type	Size	Default
ipv4-address-type	IPv4 address type.	option	-	not-available



Parameter	Description	Type	Size	Default																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>not-available</i></td><td>Address type not available.</td></tr><tr><td><i>public</i></td><td>Public IPv4 address available.</td></tr><tr><td><i>port-restricted</i></td><td>Port-restricted IPv4 address available.</td></tr><tr><td><i>single-NATed-private</i></td><td>Single NATed private IPv4 address available.</td></tr><tr><td><i>double-NATed-private</i></td><td>Double NATed private IPv4 address available.</td></tr><tr><td><i>port-restricted-and-single-NATed</i></td><td>Port-restricted IPv4 address and single NATed IPv4 address available.</td></tr><tr><td><i>port-restricted-and-double-NATed</i></td><td>Port-restricted IPv4 address and double NATed IPv4 address available.</td></tr><tr><td><i>not-known</i></td><td>Availability of the address type is not known.</td></tr></table>	Option	Description	<i>not-available</i>	Address type not available.	<i>public</i>	Public IPv4 address available.	<i>port-restricted</i>	Port-restricted IPv4 address available.	<i>single-NATed-private</i>	Single NATed private IPv4 address available.	<i>double-NATed-private</i>	Double NATed private IPv4 address available.	<i>port-restricted-and-single-NATed</i>	Port-restricted IPv4 address and single NATed IPv4 address available.	<i>port-restricted-and-double-NATed</i>	Port-restricted IPv4 address and double NATed IPv4 address available.	<i>not-known</i>	Availability of the address type is not known.			
	Option	Description																				
	<i>not-available</i>	Address type not available.																				
	<i>public</i>	Public IPv4 address available.																				
	<i>port-restricted</i>	Port-restricted IPv4 address available.																				
	<i>single-NATed-private</i>	Single NATed private IPv4 address available.																				
	<i>double-NATed-private</i>	Double NATed private IPv4 address available.																				
	<i>port-restricted-and-single-NATed</i>	Port-restricted IPv4 address and single NATed IPv4 address available.																				
	<i>port-restricted-and-double-NATed</i>	Port-restricted IPv4 address and double NATed IPv4 address available.																				
<i>not-known</i>	Availability of the address type is not known.																					
ipv6-address-type	IPv6 address type.	option	-	not-available																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>not-available</i></td><td>Address type not available.</td></tr><tr><td><i>available</i></td><td>Address type available.</td></tr><tr><td><i>not-known</i></td><td>Availability of the address type not known.</td></tr></table>	Option	Description	<i>not-available</i>	Address type not available.	<i>available</i>	Address type available.	<i>not-known</i>	Availability of the address type not known.													
	Option	Description																				
	<i>not-available</i>	Address type not available.																				
	<i>available</i>	Address type available.																				
<i>not-known</i>	Availability of the address type not known.																					
name	IP type name.	string	Maximum length: 35																			

## config wireless-controller hotspot20 anqp-nai-realm

Configure network access identifier (NAI) realm.

```

config wireless-controller hotspot20 anqp-nai-realm
  Description: Configure network access identifier (NAI) realm.
  edit <name>
    config nai-list
      Description: NAI list.
      edit <name>
        set encoding [disable|enable]
        set nai-realm {string}
      config eap-method
        Description: EAP Methods.
        edit <index>
          set method [eap-identity|eap-md5|...]

```

```

        config auth-param
        Description: EAP auth param.
        edit <index>
        set id [non-eap-inner-auth|inner-auth-eap|...]
        set val [eap-identity|eap-md5|...]
        next
    end
next
end
next
end
next
end
next
end

```

## config wireless-controller hotspot20 anqp-nai-realm

Parameter	Description	Type	Size	Default
name	NAI realm list name.	string	Maximum length: 35	

## config nai-list

Parameter	Description	Type	Size	Default
name	NAI realm name.	string	Maximum length: 35	
encoding	Enable/disable format in accordance with IETF RFC 4282.	option	-	enable
	Option	Description		
	disable	Disable format in accordance with IETF RFC 4282.		
	enable	Enable format in accordance with IETF RFC 4282.		
nai-realm	Configure NAI realms (delimited by a semi-colon character).	string	Maximum length: 255	

## config eap-method

Parameter	Description	Type	Size	Default
index	EAP method index.	integer	Minimum value: 1 Maximum value: 5	0
method	EAP method type.	option	-	eap-identity

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>eap-identity</i>	Identity.		
	<i>eap-md5</i>	MD5.		
	<i>eap-tls</i>	TLS.		
	<i>eap-ttls</i>	TTLS.		
	<i>eap-peap</i>	PEAP.		
	<i>eap-sim</i>	SIM.		
	<i>eap-aka</i>	AKA.		
	<i>eap-aka-prime</i>	AKA'.		

### config auth-param

Parameter	Description	Type	Size	Default
index	Param index.	integer	Minimum value: 1 Maximum value: 4	0
id	ID of authentication parameter.	option	-	inner-auth-eap
	<b>Option</b>	<b>Description</b>		
	<i>non-eap-inner-auth</i>	Non-EAP inner authentication type.		
	<i>inner-auth-eap</i>	Inner authentication EAP method type.		
	<i>credential</i>	Credential type.		
	<i>tunneled-credential</i>	Tunneled EAP method credential type.		
val	Value of authentication parameter.	option	-	eap-identity
	<b>Option</b>	<b>Description</b>		
	<i>eap-identity</i>	EAP Identity.		
	<i>eap-md5</i>	EAP MD5.		
	<i>eap-tls</i>	EAP TLS.		
	<i>eap-ttls</i>	EAP TTLS.		

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>eap-peap</i>	EAP PEAP.		
	<i>eap-sim</i>	EAP SIM.		
	<i>eap-aka</i>	EAP AKA.		
	<i>eap-aka-prime</i>	EAP AKA'.		
	<i>non-eap-pap</i>	Non EAP PAP.		
	<i>non-eap-chap</i>	Non EAP CHAP.		
	<i>non-eap-mschap</i>	Non EAP MSCHAP.		
	<i>non-eap-mschapv2</i>	Non EAP MSCHAPV2.		
	<i>cred-sim</i>	Credential SIM.		
	<i>cred-usim</i>	Credential USIM.		
	<i>cred-nfc</i>	Credential NFC secure element.		
	<i>cred-hardware-token</i>	Credential hardware token.		
	<i>cred-softoken</i>	Credential softoken.		
	<i>cred-certificate</i>	Credential certificate.		
	<i>cred-user-pwd</i>	Credential username password.		
	<i>cred-none</i>	Credential none.		
	<i>cred-vendor-specific</i>	Credential vendor specific.		
	<i>tun-cred-sim</i>	Tunneled credential SIM.		
	<i>tun-cred-usim</i>	Tunneled credential USIM.		
	<i>tun-cred-nfc</i>	Tunneled credential NFC secure element.		
	<i>tun-cred-hardware-token</i>	Tunneled credential hardware token.		
	<i>tun-cred-softoken</i>	Tunneled credential softoken.		
	<i>tun-cred-certificate</i>	Tunneled credential certificate.		
	<i>tun-cred-user-pwd</i>	Tunneled credential username password.		

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>tun-cred-anonymous</i>	Tunneled credential anonymous.		
	<i>tun-cred-vendor-specific</i>	Tunneled credential vendor specific.		

## config wireless-controller hotspot20 anqp-network-auth-type

Configure network authentication type.

```
config wireless-controller hotspot20 anqp-network-auth-type
  Description: Configure network authentication type.
  edit <name>
    set auth-type [acceptance-of-terms|online-enrollment|...]
    set url {string}
  next
end
```

## config wireless-controller hotspot20 anqp-network-auth-type

Parameter	Description	Type	Size	Default
auth-type	Network authentication type.	option	-	acceptance-of-terms
	<b>Option</b>	<b>Description</b>		
	<i>acceptance-of-terms</i>	Acceptance of terms and conditions.		
	<i>online-enrollment</i>	Online enrollment supported.		
	<i>http-redirection</i>	HTTP and HTTPS redirection.		
	<i>dns-redirection</i>	DNS redirection.		
name	Authentication type name.	string	Maximum length: 35	
url	Redirect URL.	string	Maximum length: 255	

## config wireless-controller hotspot20 anqp-roaming-consortium

Configure roaming consortium.

```

config wireless-controller hotspot20 anqp-roaming-consortium
  Description: Configure roaming consortium.
  edit <name>
    config oi-list
      Description: Organization identifier list.
      edit <index>
        set oi {string}
        set comment {string}
      next
    end
  next
end

```

## config wireless-controller hotspot20 anqp-roaming-consortium

Parameter	Description	Type	Size	Default
name	Roaming consortium name.	string	Maximum length: 35	

## config oi-list

Parameter	Description	Type	Size	Default
index	OI index.	integer	Minimum value: 1 Maximum value: 10	0
oi	Organization identifier.	string	Maximum length: 10	
comment	Comment.	string	Maximum length: 35	

## config wireless-controller hotspot20 anqp-venue-name

Configure venue name duple.

```

config wireless-controller hotspot20 anqp-venue-name
  Description: Configure venue name duple.
  edit <name>
    config value-list
      Description: Name list.
      edit <index>
        set lang {string}
        set value {string}
      next
    end
  next
end

```

## config wireless-controller hotspot20 anqp-venue-name

Parameter	Description	Type	Size	Default
name	Name of venue name duple.	string	Maximum length: 35	

## config value-list

Parameter	Description	Type	Size	Default
index	Value index.	integer	Minimum value: 1 Maximum value: 10	0
lang	Language code.	string	Maximum length: 3	eng
value	Venue name value.	string	Maximum length: 252	

## config wireless-controller hotspot20 anqp-venue-url

Configure venue URL.

```
config wireless-controller hotspot20 anqp-venue-url
  Description: Configure venue URL.
  edit <name>
    config value-list
      Description: URL list.
      edit <index>
        set number {integer}
        set value {string}
      next
    end
  next
end
```

## config wireless-controller hotspot20 anqp-venue-url

Parameter	Description	Type	Size	Default
name	Name of venue url.	string	Maximum length: 35	

## config value-list

Parameter	Description	Type	Size	Default
index	URL index.	integer	Minimum value: 1 Maximum value: 10	0
number	Venue number.	integer	Minimum value: 0 Maximum value: 255	0
value	Venue URL value.	string	Maximum length: 254	

## config wireless-controller hotspot20 h2qp-advice-of-charge

Configure advice of charge.

```
config wireless-controller hotspot20 h2qp-advice-of-charge
  Description: Configure advice of charge.
  edit <name>
    config aoc-list
      Description: AOC list.
      edit <name>
        set type [time-based|volume-based|...]
        set nai-realm-encoding {string}
        set nai-realm {string}
        config plan-info
          Description: Plan info.
          edit <name>
            set lang {string}
            set currency {string}
            set info-file {string}
          next
        end
      next
    end
  next
end
```

## config wireless-controller hotspot20 h2qp-advice-of-charge

Parameter	Description	Type	Size	Default
name	Plan name.	string	Maximum length: 35	



## config aoc-list

Parameter	Description	Type	Size	Default										
name	Advice of charge ID.	string	Maximum length: 35											
type	Usage charge type.	option	-	time-based										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>time-based</i></td><td>Time based usage charge.</td></tr><tr><td><i>volume-based</i></td><td>Volume based usage charge.</td></tr><tr><td><i>time-and-volume-based</i></td><td>Time and volume based usage charge.</td></tr><tr><td><i>unlimited</i></td><td>Unlimited usage.</td></tr></table>				Option	Description	<i>time-based</i>	Time based usage charge.	<i>volume-based</i>	Volume based usage charge.	<i>time-and-volume-based</i>	Time and volume based usage charge.	<i>unlimited</i>	Unlimited usage.
	Option	Description												
	<i>time-based</i>	Time based usage charge.												
	<i>volume-based</i>	Volume based usage charge.												
	<i>time-and-volume-based</i>	Time and volume based usage charge.												
<i>unlimited</i>	Unlimited usage.													
nai-realm-encoding	NAI realm encoding.	string	Maximum length: 1											
nai-realm	NAI realm list name.	string	Maximum length: 255											

## config plan-info

Parameter	Description	Type	Size	Default
name	Plan name.	string	Maximum length: 35	
lang	Language code.	string	Maximum length: 3	
currency	Currency code.	string	Maximum length: 3	
info-file	Info file.	string	Maximum length: 64	

## config wireless-controller hotspot20 h2qp-conn-capability

Configure connection capability.

```
config wireless-controller hotspot20 h2qp-conn-capability
  Description: Configure connection capability.
  edit <name>
    set esp-port [closed|open|...]
    set ftp-port [closed|open|...]
    set http-port [closed|open|...]
    set icmp-port [closed|open|...]
```

```

set ikev2-port [closed|open|...]
set ikev2-xx-port [closed|open|...]
set pptp-vpn-port [closed|open|...]
set ssh-port [closed|open|...]
set tls-port [closed|open|...]
set voip-tcp-port [closed|open|...]
set voip-udp-port [closed|open|...]
next
end

```

## config wireless-controller hotspot20 h2qp-conn-capability

Parameter	Description	Type	Size	Default
esp-port	Set ESP port service (used by IPsec VPNs) status.	option	-	unknown
	<b>Option</b>	<b>Description</b>		
	<i>closed</i>	The port is not open for communication.		
	<i>open</i>	The port is open for communication.		
	<i>unknown</i>	The port may or may not be open for communication.		
ftp-port	Set FTP port service status.	option	-	unknown
	<b>Option</b>	<b>Description</b>		
	<i>closed</i>	The port is not open for communication.		
	<i>open</i>	The port is open for communication.		
	<i>unknown</i>	The port may or may not be open for communication.		
http-port	Set HTTP port service status.	option	-	unknown
	<b>Option</b>	<b>Description</b>		
	<i>closed</i>	The port is not open for communication.		
	<i>open</i>	The port is open for communication.		
	<i>unknown</i>	The port may or may not be open for communication.		
icmp-port	Set ICMP port service status.	option	-	unknown
	<b>Option</b>	<b>Description</b>		
	<i>closed</i>	The port is not open for communication.		
	<i>open</i>	The port is open for communication.		
	<i>unknown</i>	The port may or may not be open for communication.		
ikev2-port	Set IKEv2 port service for IPsec VPN status.	option	-	unknown

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>closed</i>	The port is not open for communication.		
	<i>open</i>	The port is open for communication.		
	<i>unknown</i>	The port may or may not be open for communication.		
ikev2-xx-port	Set UDP port 4500 (which may be used by IKEv2 for IPsec VPN) service status.	option	-	unknown
	<b>Option</b>	<b>Description</b>		
	<i>closed</i>	The port is not open for communication.		
	<i>open</i>	The port is open for communication.		
	<i>unknown</i>	The port may or may not be open for communication.		
name	Connection capability name.	string	Maximum length: 35	
pptp-vpn-port	Set Point to Point Tunneling Protocol (PPTP) VPN port service status.	option	-	unknown
	<b>Option</b>	<b>Description</b>		
	<i>closed</i>	The port is not open for communication.		
	<i>open</i>	The port is open for communication.		
	<i>unknown</i>	The port may or may not be open for communication.		
ssh-port	Set SSH port service status.	option	-	unknown
	<b>Option</b>	<b>Description</b>		
	<i>closed</i>	The port is not open for communication.		
	<i>open</i>	The port is open for communication.		
	<i>unknown</i>	The port may or may not be open for communication.		
tls-port	Set TLS VPN (HTTPS) port service status.	option	-	unknown
	<b>Option</b>	<b>Description</b>		
	<i>closed</i>	The port is not open for communication.		
	<i>open</i>	The port is open for communication.		
	<i>unknown</i>	The port may or may not be open for communication.		
voip-tcp-port	Set VoIP TCP port service status.	option	-	unknown

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>closed</i>	The port is not open for communication.		
	<i>open</i>	The port is open for communication.		
	<i>unknown</i>	The port may or may not be open for communication.		
voip-udp-port	Set VoIP UDP port service status.	option	-	unknown
	<b>Option</b>	<b>Description</b>		
	<i>closed</i>	The port is not open for communication.		
	<i>open</i>	The port is open for communication.		
	<i>unknown</i>	The port may or may not be open for communication.		

## config wireless-controller hotspot20 h2qp-operator-name

Configure operator friendly name.

```
config wireless-controller hotspot20 h2qp-operator-name
  Description: Configure operator friendly name.
  edit <name>
    config value-list
      Description: Name list.
      edit <index>
        set lang {string}
        set value {string}
      next
    end
  next
end
```

## config wireless-controller hotspot20 h2qp-operator-name

Parameter	Description	Type	Size	Default
name	Friendly name ID.	string	Maximum length: 35	

## config value-list

Parameter	Description	Type	Size	Default
index	Value index.	integer	Minimum value: 1 Maximum value: 10	0
lang	Language code.	string	Maximum length: 3	eng
value	Friendly name value.	string	Maximum length: 252	

## config wireless-controller hotspot20 h2qp-osu-provider-nai

Configure online sign up (OSU) provider NAI list.

```
config wireless-controller hotspot20 h2qp-osu-provider-nai
  Description: Configure online sign up (OSU) provider NAI list.
  edit <name>
    config nai-list
      Description: OSU NAI list.
      edit <name>
        set osu-nai {string}
      next
    end
  next
end
```

## config wireless-controller hotspot20 h2qp-osu-provider-nai

Parameter	Description	Type	Size	Default
name	OSU provider NAI ID.	string	Maximum length: 35	

## config nai-list

Parameter	Description	Type	Size	Default
name	OSU NAI ID.	string	Maximum length: 35	
osu-nai	OSU NAI.	string	Maximum length: 255	

## config wireless-controller hotspot20 h2qp-osu-provider

Configure online sign up (OSU) provider list.

```
config wireless-controller hotspot20 h2qp-osu-provider
  Description: Configure online sign up (OSU) provider list.
  edit <name>
    config friendly-name
      Description: OSU provider friendly name.
      edit <index>
        set lang {string}
        set friendly-name {string}
      next
    end
    set icon {string}
    set osu-method {option1}, {option2}, ...
    set osu-nai {string}
    set server-uri {string}
    config service-description
      Description: OSU service name.
      edit <service-id>
        set lang {string}
        set service-description {string}
      next
    end
  next
end
```

## config wireless-controller hotspot20 h2qp-osu-provider

Parameter	Description	Type	Size	Default
icon	OSU provider icon.	string	Maximum length: 35	
name	OSU provider ID.	string	Maximum length: 35	
osu-method	OSU method list.	option	-	
	<b>Option</b>	<b>Description</b>		
	<i>oma-dm</i>	OMA DM.		
	<i>soap-xml-spp</i>	SOAP XML SPP.		
	<i>reserved</i>	Reserved.		
osu-nai	OSU NAI.	string	Maximum length: 255	
server-uri	Server URI.	string	Maximum length: 255	

## config friendly-name

Parameter	Description	Type	Size	Default
index	OSU provider friendly name index.	integer	Minimum value: 1 Maximum value: 10	0
lang	Language code.	string	Maximum length: 3	eng
friendly-name	OSU provider friendly name.	string	Maximum length: 252	

## config service-description

Parameter	Description	Type	Size	Default
service-id	OSU service ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
lang	Language code.	string	Maximum length: 3	eng
service-description	Service description.	string	Maximum length: 252	

## config wireless-controller hotspot20 h2qp-terms-and-conditions

Configure terms and conditions.

```
config wireless-controller hotspot20 h2qp-terms-and-conditions
  Description: Configure terms and conditions.
  edit <name>
    set filename {string}
    set timestamp {integer}
    set url {string}
  next
end
```

## config wireless-controller hotspot20 h2qp-terms-and-conditions

Parameter	Description	Type	Size	Default
filename	Filename.	string	Maximum length: 254	

Parameter	Description	Type	Size	Default
name	Terms and Conditions ID.	string	Maximum length: 35	
timestamp	Timestamp.	integer	Minimum value: 0 Maximum value: 4294967295	0
url	URL.	string	Maximum length: 253	

## config wireless-controller hotspot20 h2qp-wan-metric

Configure WAN metrics.

```
config wireless-controller hotspot20 h2qp-wan-metric
  Description: Configure WAN metrics.
  edit <name>
    set downlink-load {integer}
    set downlink-speed {integer}
    set link-at-capacity [enable|disable]
    set link-status [up|down|...]
    set load-measurement-duration {integer}
    set symmetric-wan-link [symmetric|asymmetric]
    set uplink-load {integer}
    set uplink-speed {integer}
  next
end
```

## config wireless-controller hotspot20 h2qp-wan-metric

Parameter	Description	Type	Size	Default
downlink-load	Downlink load.	integer	Minimum value: 0 Maximum value: 255	0
downlink-speed	Downlink speed (in kilobits/s).	integer	Minimum value: 0 Maximum value: 4294967295	2400
link-at-capacity	Link at capacity.	option	-	disable



Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Link at capacity (not allow additional mobile devices to associate).		
	<i>disable</i>	Link not at capacity (allow additional mobile devices to associate).		
link-status	Link status.	option	-	up
	<b>Option</b>	<b>Description</b>		
	<i>up</i>	Link up.		
	<i>down</i>	Link down.		
	<i>in-test</i>	Link in test state.		
load-measurement-duration	Load measurement duration (in tenths of a second).	integer	Minimum value: 0 Maximum value: 65535	0
name	WAN metric name.	string	Maximum length: 35	
symmetric-wan-link	WAN link symmetry.	option	-	asymmetric
	<b>Option</b>	<b>Description</b>		
	<i>symmetric</i>	Symmetric WAN link (uplink and downlink speeds are the same).		
	<i>asymmetric</i>	Asymmetric WAN link (uplink and downlink speeds are not the same).		
uplink-load	Uplink load.	integer	Minimum value: 0 Maximum value: 255	0
uplink-speed	Uplink speed (in kilobits/s).	integer	Minimum value: 0 Maximum value: 4294967295	2400

## config wireless-controller hotspot20 hs-profile

Configure hotspot profile.

```
config wireless-controller hotspot20 hs-profile
  Description: Configure hotspot profile.
  edit <name>
    set 3gpp-plmn {string}
    set access-network-asra [enable|disable]
```

```

set access-network-esr [enable|disable]
set access-network-internet [enable|disable]
set access-network-type [private-network|private-network-with-guest-access|...]
set access-network-uesa [enable|disable]
set advice-of-charge {string}
set anqp-domain-id {integer}
set bss-transition [enable|disable]
set conn-cap {string}
set deauth-request-timeout {integer}
set dgaf [enable|disable]
set domain-name {string}
set gas-comeback-delay {integer}
set gas-fragmentation-limit {integer}
set hessid {mac-address}
set ip-addr-type {string}
set l2tif [enable|disable]
set nai-realm {string}
set network-auth {string}
set oper-friendly-name {string}
set oper-icon {string}
set osu-provider <name1>, <name2>, ...
set osu-provider-nai {string}
set osu-ssid {string}
set pame-bi [disable|enable]
set proxy-arp [enable|disable]
set qos-map {string}
set release {integer}
set roaming-consortium {string}
set terms-and-conditions {string}
set venue-group [unspecified|assembly|...]
set venue-name {string}
set venue-type [unspecified|arena|...]
set venue-url {string}
set wan-metrics {string}
set wnm-sleep-mode [enable|disable]
next
end

```

## config wireless-controller hotspot20 hs-profile

Parameter	Description	Type	Size	Default
3gpp-plmn	3GPP PLMN name.	string	Maximum length: 35	
access-network-asra	Enable/disable additional step required for access (ASRA).	option	-	disable
		Option	Description	
		<i>enable</i>	Enable additional step required for access (ASRA).	
		<i>disable</i>	Disable additional step required for access (ASRA).	

Parameter	Description	Type	Size	Default
access-network-esr	Enable/disable emergency services reachable (ESR).	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable emergency services reachable (ESR).		
	<i>disable</i>	Disable emergency services reachable (ESR).		
access-network-internet	Enable/disable connectivity to the Internet.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable connectivity to the Internet.		
	<i>disable</i>	Disable connectivity to the Internet.		
access-network-type	Access network type.	option	-	private-network
	<b>Option</b>	<b>Description</b>		
	<i>private-network</i>	Private network.		
	<i>private-network-with-guest-access</i>	Private network with guest access.		
	<i>chargeable-public-network</i>	Chargeable public network.		
	<i>free-public-network</i>	Free public network.		
	<i>personal-device-network</i>	Personal devices network.		
	<i>emergency-services-only-network</i>	Emergency services only network.		
	<i>test-or-experimental</i>	Test or experimental.		
	<i>wildcard</i>	Wildcard.		
access-network-uesa	Enable/disable unauthenticated emergency service accessible (UESA).	option	-	disable

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable unauthenticated emergency service accessible (UESA).		
	<i>disable</i>	Disable unauthenticated emergency service accessible (UESA).		
advice-of-charge	Advice of charge.	string	Maximum length: 35	
anqp-domain-id	ANQP Domain ID.	integer	Minimum value: 0 Maximum value: 65535	0
bss-transition	Enable/disable basic service set (BSS) transition Support.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable basic service set (BSS) transition support.		
	<i>disable</i>	Disable basic service set (BSS) transition support.		
conn-cap	Connection capability name.	string	Maximum length: 35	
deauth-request-timeout	Deauthentication request timeout (in seconds).	integer	Minimum value: 30 Maximum value: 120	60
dgaf	Enable/disable downstream group-addressed forwarding (DGAF).	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable downstream group-addressed forwarding (DGAF).		
	<i>disable</i>	Disable downstream group-addressed forwarding (DGAF).		
domain-name	Domain name.	string	Maximum length: 255	
gas-comeback-delay	GAS comeback delay.	integer	Minimum value: 100 Maximum value: 10000	500

Parameter	Description	Type	Size	Default						
gas-fragmentation-limit	GAS fragmentation limit.	integer	Minimum value: 512 Maximum value: 4096	1024						
hessid	Homogeneous extended service set identifier (HESSID).	mac-address	Not Specified	00:00:00:00:00:00						
ip-addr-type	IP address type name.	string	Maximum length: 35							
l2tif	Enable/disable Layer 2 traffic inspection and filtering.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Layer 2 traffic inspection and filtering.</td></tr><tr><td><i>disable</i></td><td>Disable Layer 2 traffic inspection and filtering.</td></tr></table>				Option	Description	<i>enable</i>	Enable Layer 2 traffic inspection and filtering.	<i>disable</i>	Disable Layer 2 traffic inspection and filtering.
Option	Description									
<i>enable</i>	Enable Layer 2 traffic inspection and filtering.									
<i>disable</i>	Disable Layer 2 traffic inspection and filtering.									
nai-realm	NAI realm list name.	string	Maximum length: 35							
name	Hotspot profile name.	string	Maximum length: 35							
network-auth	Network authentication name.	string	Maximum length: 35							
oper-friendly-name	Operator friendly name.	string	Maximum length: 35							
oper-icon	Operator icon.	string	Maximum length: 35							
osu-provider <name>	Manually selected list of OSU provider(s). OSU provider name.	string	Maximum length: 35							
osu-provider-nai	OSU Provider NAI.	string	Maximum length: 35							
osu-ssid	Online sign up (OSU) SSID.	string	Maximum length: 255							
pame-bi	Enable/disable Pre-Association Message Exchange BSSID Independent (PAME-BI).	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable Pre-Association Message Exchange BSSID Independent (PAME-BI).</td></tr><tr><td><i>enable</i></td><td>Enable Pre-Association Message Exchange BSSID Independent (PAME-BI).</td></tr></table>				Option	Description	<i>disable</i>	Disable Pre-Association Message Exchange BSSID Independent (PAME-BI).	<i>enable</i>	Enable Pre-Association Message Exchange BSSID Independent (PAME-BI).
Option	Description									
<i>disable</i>	Disable Pre-Association Message Exchange BSSID Independent (PAME-BI).									
<i>enable</i>	Enable Pre-Association Message Exchange BSSID Independent (PAME-BI).									

Parameter	Description	Type	Size	Default
proxy-arp	Enable/disable Proxy ARP.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable Proxy ARP.		
	<i>disable</i>	Disable Proxy ARP.		
qos-map	QoS MAP set ID.	string	Maximum length: 35	
release	Hotspot 2.0 Release number.	integer	Minimum value: 1 Maximum value: 3	2
roaming-consortium	Roaming consortium list name.	string	Maximum length: 35	
terms-and-conditions	Terms and conditions.	string	Maximum length: 35	
venue-group	Venue group.	option	-	unspecified
	<b>Option</b>	<b>Description</b>		
	<i>unspecified</i>	Unspecified.		
	<i>assembly</i>	Assembly.		
	<i>business</i>	Business.		
	<i>educational</i>	Educational.		
	<i>factory</i>	Factory and industrial.		
	<i>institutional</i>	Institutional.		
	<i>mercantile</i>	Mercantile.		
	<i>residential</i>	Residential.		
	<i>storage</i>	Storage.		
	<i>utility</i>	Utility and miscellaneous.		
	<i>vehicular</i>	Vehicular.		
	<i>outdoor</i>	Outdoor.		
venue-name	Venue name.	string	Maximum length: 35	
venue-type	Venue type.	option	-	unspecified

Parameter	Description	Type	Size	Default
-----------	-------------	------	------	---------

Option	Description
<i>unspecified</i>	Unspecified.
<i>arena</i>	Arena.
<i>stadium</i>	Stadium.
<i>passenger-terminal</i>	Passenger terminal.
<i>amphitheater</i>	Amphitheater.
<i>amusement-park</i>	Amusement park.
<i>place-of-worship</i>	Place of worship.
<i>convention-center</i>	Convention center.
<i>library</i>	Library.
<i>museum</i>	Museum.
<i>restaurant</i>	Restaurant.
<i>theater</i>	Theater.
<i>bar</i>	Bar.
<i>coffee-shop</i>	Coffee shop.
<i>zoo-or-aquarium</i>	Zoo or aquarium.
<i>emergency-center</i>	Emergency coordination center.
<i>doctor-office</i>	Doctor or dentist office.
<i>bank</i>	Bank.
<i>fire-station</i>	Fire station.
<i>police-station</i>	Police station.
<i>post-office</i>	Post office.
<i>professional-office</i>	Professional office.
<i>research-facility</i>	Research and development facility.
<i>attorney-office</i>	Attorney office.
<i>primary-school</i>	Primary school.

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>secondary-school</i>	Secondary school.		
	<i>university-or-college</i>	University or college.		
	<i>factory</i>	Factory.		
	<i>hospital</i>	Hospital.		
	<i>long-term-care-facility</i>	Long term care facility.		
	<i>rehab-center</i>	Alcohol and drug rehabilitation center.		
	<i>group-home</i>	Group home.		
	<i>prison-or-jail</i>	Prison or jail.		
	<i>retail-store</i>	Retail store.		
	<i>grocery-market</i>	Grocery market.		
	<i>auto-service-station</i>	Auto service station.		
	<i>shopping-mall</i>	Shopping mall.		
	<i>gas-station</i>	Gas station.		
	<i>private</i>	Private residence.		
	<i>hotel-or-motel</i>	Hotel or motel.		
	<i>dormitory</i>	Dormitory.		
	<i>boarding-house</i>	Boarding house.		
	<i>automobile</i>	Automobile or truck.		
	<i>airplane</i>	Airplane.		
	<i>bus</i>	Bus.		
	<i>ferry</i>	Ferry.		
	<i>ship-or-boat</i>	Ship or boat.		
	<i>train</i>	Train.		
	<i>motor-bike</i>	Motor bike.		
	<i>muni-mesh-network</i>	Muni mesh network.		



Parameter	Description	Type	Size	Default												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>city-park</i></td><td>City park.</td></tr><tr><td><i>rest-area</i></td><td>Rest area.</td></tr><tr><td><i>traffic-control</i></td><td>Traffic control.</td></tr><tr><td><i>bus-stop</i></td><td>Bus stop.</td></tr><tr><td><i>kiosk</i></td><td>Kiosk.</td></tr></table>	Option	Description	<i>city-park</i>	City park.	<i>rest-area</i>	Rest area.	<i>traffic-control</i>	Traffic control.	<i>bus-stop</i>	Bus stop.	<i>kiosk</i>	Kiosk.			
	Option	Description														
	<i>city-park</i>	City park.														
	<i>rest-area</i>	Rest area.														
	<i>traffic-control</i>	Traffic control.														
	<i>bus-stop</i>	Bus stop.														
<i>kiosk</i>	Kiosk.															
venue-url	Venue name.	string	Maximum length: 35													
wan-metrics	WAN metric name.	string	Maximum length: 35													
wnm-sleep-mode	Enable/disable wireless network management (WNM) sleep mode.	option	-	disable												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable wireless network management (WNM) sleep mode.</td></tr><tr><td><i>disable</i></td><td>Disable wireless network management (WNM) sleep mode.</td></tr></table>	Option	Description	<i>enable</i>	Enable wireless network management (WNM) sleep mode.	<i>disable</i>	Disable wireless network management (WNM) sleep mode.									
	Option	Description														
	<i>enable</i>	Enable wireless network management (WNM) sleep mode.														
<i>disable</i>	Disable wireless network management (WNM) sleep mode.															

## config wireless-controller hotspot20 icon

Configure OSU provider icon.

```

config wireless-controller hotspot20 icon
  Description: Configure OSU provider icon.
  edit <name>
    config icon-list
      Description: Icon list.
      edit <name>
        set lang {string}
        set file {string}
        set type [bmp|gif|...]
        set width {integer}
        set height {integer}
      next
    end
  next
end

```

## config wireless-controller hotspot20 icon

Parameter	Description	Type	Size	Default
name	Icon list ID.	string	Maximum length: 35	

## config icon-list

Parameter	Description	Type	Size	Default												
name	Icon name.	string	Maximum length: 255													
lang	Language code.	string	Maximum length: 3	eng												
file	Icon file.	string	Maximum length: 255													
type	Icon type.	option	-	png												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>bmp</i></td><td>BMP image.</td></tr><tr><td><i>gif</i></td><td>GIF image.</td></tr><tr><td><i>jpeg</i></td><td>JPEG image.</td></tr><tr><td><i>png</i></td><td>PNG image.</td></tr><tr><td><i>tiff</i></td><td>TIFF image.</td></tr></table>				Option	Description	<i>bmp</i>	BMP image.	<i>gif</i>	GIF image.	<i>jpeg</i>	JPEG image.	<i>png</i>	PNG image.	<i>tiff</i>	TIFF image.
	Option	Description														
	<i>bmp</i>	BMP image.														
	<i>gif</i>	GIF image.														
	<i>jpeg</i>	JPEG image.														
	<i>png</i>	PNG image.														
<i>tiff</i>	TIFF image.															
width	Icon width.	integer	Minimum value: 1 Maximum value: 65535	0												
height	Icon height.	integer	Minimum value: 1 Maximum value: 65535	0												

## config wireless-controller hotspot20 qos-map

Configure QoS map set.

```
config wireless-controller hotspot20 qos-map
  Description: Configure QoS map set.
  edit <name>
```

```

config dscp-except
    Description: Differentiated Services Code Point (DSCP) exceptions.
    edit <index>
        set dscp {integer}
        set up {integer}
    next
end
config dscp-range
    Description: Differentiated Services Code Point (DSCP) ranges.
    edit <index>
        set up {integer}
        set low {integer}
        set high {integer}
    next
end
next
end

```

## config wireless-controller hotspot20 qos-map

Parameter	Description	Type	Size	Default
name	QOS-MAP name.	string	Maximum length: 35	

## config dscp-except

Parameter	Description	Type	Size	Default
index	DSCP exception index.	integer	Minimum value: 1 Maximum value: 21	0
dscp	DSCP value.	integer	Minimum value: 0 Maximum value: 63	0
up	User priority.	integer	Minimum value: 0 Maximum value: 7	0

## config dscp-range

Parameter	Description	Type	Size	Default
index	DSCP range index.	integer	Minimum value: 1 Maximum value: 8	0
up	User priority.	integer	Minimum value: 0 Maximum value: 7	0
low	DSCP low value.	integer	Minimum value: 0 Maximum value: 63	255
high	DSCP high value.	integer	Minimum value: 0 Maximum value: 63	255

## config wireless-controller inter-controller

Configure inter wireless controller operation.

```
config wireless-controller inter-controller
  Description: Configure inter wireless controller operation.
  set fast-failover-max {integer}
  set fast-failover-wait {integer}
  set inter-controller-key {password}
  set inter-controller-mode [disable|l2-roaming|...]
  config inter-controller-peer
    Description: Fast failover peer wireless controller list.
    edit <id>
      set peer-ip {ipv4-address}
      set peer-port {integer}
      set peer-priority [primary|secondary]
    next
  end
  set inter-controller-pri [primary|secondary]
end
```

## config wireless-controller inter-controller

Parameter	Description	Type	Size	Default								
fast-failover-max	Maximum number of retransmissions for fast failover HA messages between peer wireless controllers.	integer	Minimum value: 3 Maximum value: 64	10								
fast-failover-wait	Minimum wait time before an AP transitions from secondary controller to primary controller.	integer	Minimum value: 10 Maximum value: 86400	10								
inter-controller-key	Secret key for inter-controller communications.	password	Not Specified									
inter-controller-mode	Configure inter-controller mode.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable inter-controller mode.</td></tr><tr><td>l2-roaming</td><td>Enable layer 2 roaming support between inter-controllers.</td></tr><tr><td>1+1</td><td>Enable 1+1 fast failover mode.</td></tr></table>				Option	Description	disable	Disable inter-controller mode.	l2-roaming	Enable layer 2 roaming support between inter-controllers.	1+1	Enable 1+1 fast failover mode.
	Option	Description										
	disable	Disable inter-controller mode.										
	l2-roaming	Enable layer 2 roaming support between inter-controllers.										
1+1	Enable 1+1 fast failover mode.											
inter-controller-pri	Configure inter-controller's priority.	option	-	primary								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>primary</td><td>Primary fast failover mode.</td></tr><tr><td>secondary</td><td>Secondary fast failover mode.</td></tr></table>				Option	Description	primary	Primary fast failover mode.	secondary	Secondary fast failover mode.		
	Option	Description										
	primary	Primary fast failover mode.										
secondary	Secondary fast failover mode.											

## config inter-controller-peer

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
peer-ip	Peer wireless controller's IP address.	ipv4-address	Not Specified	0.0.0.0

Parameter	Description	Type	Size	Default						
peer-port	Port used by the wireless controller's for inter-controller communications.	integer	Minimum value: 1024 Maximum value: 49150	5246						
peer-priority	Peer wireless controller's priority.	option	-	primary						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>primary</i></td><td>Primary fast failover mode.</td></tr><tr><td><i>secondary</i></td><td>Secondary fast failover mode.</td></tr></table>				Option	Description	<i>primary</i>	Primary fast failover mode.	<i>secondary</i>	Secondary fast failover mode.
Option	Description									
<i>primary</i>	Primary fast failover mode.									
<i>secondary</i>	Secondary fast failover mode.									

## config wireless-controller log

Configure wireless controller event log filters.

```
config wireless-controller log
    Description: Configure wireless controller event log filters.
    set addrgrp-log [emergency|alert|...]
    set ble-log [emergency|alert|...]
    set clb-log [emergency|alert|...]
    set dhcp-starv-log [emergency|alert|...]
    set led-sched-log [emergency|alert|...]
    set radio-event-log [emergency|alert|...]
    set rogue-event-log [emergency|alert|...]
    set sta-event-log [emergency|alert|...]
    set sta-locate-log [emergency|alert|...]
    set status [enable|disable]
    set wids-log [emergency|alert|...]
    set wtp-event-log [emergency|alert|...]
end
```

## config wireless-controller log

Parameter	Description	Type	Size	Default												
addrgrp-log	Lowest severity level to log address group message.	option	-	notification												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>emergency</i></td><td>Emergency level.</td></tr><tr><td><i>alert</i></td><td>Alert level.</td></tr><tr><td><i>critical</i></td><td>Critical level.</td></tr><tr><td><i>error</i></td><td>Error level.</td></tr><tr><td><i>warning</i></td><td>Warning level.</td></tr></table>				Option	Description	<i>emergency</i>	Emergency level.	<i>alert</i>	Alert level.	<i>critical</i>	Critical level.	<i>error</i>	Error level.	<i>warning</i>	Warning level.
	Option	Description														
	<i>emergency</i>	Emergency level.														
	<i>alert</i>	Alert level.														
	<i>critical</i>	Critical level.														
	<i>error</i>	Error level.														
<i>warning</i>	Warning level.															

Parameter	Description	Type	Size	Default																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>notification</i></td><td>Notification level.</td></tr><tr><td><i>information</i></td><td>Information level.</td></tr><tr><td><i>debug</i></td><td>Debug level.</td></tr></table>	Option	Description	<i>notification</i>	Notification level.	<i>information</i>	Information level.	<i>debug</i>	Debug level.													
	Option	Description																				
	<i>notification</i>	Notification level.																				
	<i>information</i>	Information level.																				
<i>debug</i>	Debug level.																					
ble-log	Lowest severity level to log BLE detection message.	option	-	notification																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>emergency</i></td><td>Emergency level.</td></tr><tr><td><i>alert</i></td><td>Alert level.</td></tr><tr><td><i>critical</i></td><td>Critical level.</td></tr><tr><td><i>error</i></td><td>Error level.</td></tr><tr><td><i>warning</i></td><td>Warning level.</td></tr><tr><td><i>notification</i></td><td>Notification level.</td></tr><tr><td><i>information</i></td><td>Information level.</td></tr><tr><td><i>debug</i></td><td>Debug level.</td></tr></table>	Option	Description	<i>emergency</i>	Emergency level.	<i>alert</i>	Alert level.	<i>critical</i>	Critical level.	<i>error</i>	Error level.	<i>warning</i>	Warning level.	<i>notification</i>	Notification level.	<i>information</i>	Information level.	<i>debug</i>	Debug level.			
	Option	Description																				
	<i>emergency</i>	Emergency level.																				
	<i>alert</i>	Alert level.																				
	<i>critical</i>	Critical level.																				
	<i>error</i>	Error level.																				
	<i>warning</i>	Warning level.																				
	<i>notification</i>	Notification level.																				
	<i>information</i>	Information level.																				
<i>debug</i>	Debug level.																					
clb-log	Lowest severity level to log client load balancing message.	option	-	notification																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>emergency</i></td><td>Emergency level.</td></tr><tr><td><i>alert</i></td><td>Alert level.</td></tr><tr><td><i>critical</i></td><td>Critical level.</td></tr><tr><td><i>error</i></td><td>Error level.</td></tr><tr><td><i>warning</i></td><td>Warning level.</td></tr><tr><td><i>notification</i></td><td>Notification level.</td></tr><tr><td><i>information</i></td><td>Information level.</td></tr><tr><td><i>debug</i></td><td>Debug level.</td></tr></table>	Option	Description	<i>emergency</i>	Emergency level.	<i>alert</i>	Alert level.	<i>critical</i>	Critical level.	<i>error</i>	Error level.	<i>warning</i>	Warning level.	<i>notification</i>	Notification level.	<i>information</i>	Information level.	<i>debug</i>	Debug level.			
	Option	Description																				
	<i>emergency</i>	Emergency level.																				
	<i>alert</i>	Alert level.																				
	<i>critical</i>	Critical level.																				
	<i>error</i>	Error level.																				
	<i>warning</i>	Warning level.																				
	<i>notification</i>	Notification level.																				
	<i>information</i>	Information level.																				
<i>debug</i>	Debug level.																					
dhcp-starv-log	Lowest severity level to log DHCP starvation event message.	option	-	notification																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>emergency</i></td><td>Emergency level.</td></tr></table>	Option	Description	<i>emergency</i>	Emergency level.																	
	Option	Description																				
<i>emergency</i>	Emergency level.																					

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>alert</i>	Alert level.		
	<i>critical</i>	Critical level.		
	<i>error</i>	Error level.		
	<i>warning</i>	Warning level.		
	<i>notification</i>	Notification level.		
	<i>information</i>	Information level.		
	<i>debug</i>	Debug level.		
led-sched-log	Lowest severity level to log LED schedule event message.	option	-	notification
	<b>Option</b>	<b>Description</b>		
	<i>emergency</i>	Emergency level.		
	<i>alert</i>	Alert level.		
	<i>critical</i>	Critical level.		
	<i>error</i>	Error level.		
	<i>warning</i>	Warning level.		
	<i>notification</i>	Notification level.		
	<i>information</i>	Information level.		
<i>debug</i>	Debug level.			
radio-event-log	Lowest severity level to log radio event message.	option	-	notification
	<b>Option</b>	<b>Description</b>		
	<i>emergency</i>	Emergency level.		
	<i>alert</i>	Alert level.		
	<i>critical</i>	Critical level.		
	<i>error</i>	Error level.		
	<i>warning</i>	Warning level.		
	<i>notification</i>	Notification level.		
	<i>information</i>	Information level.		
<i>debug</i>	Debug level.			



Parameter	Description	Type	Size	Default
rogue-event-log	Lowest severity level to log rogue AP event message.	option	-	notification
	<b>Option</b>	<b>Description</b>		
	<i>emergency</i>	Emergency level.		
	<i>alert</i>	Alert level.		
	<i>critical</i>	Critical level.		
	<i>error</i>	Error level.		
	<i>warning</i>	Warning level.		
	<i>notification</i>	Notification level.		
	<i>information</i>	Information level.		
	<i>debug</i>	Debug level.		
sta-event-log	Lowest severity level to log station event message.	option	-	notification
	<b>Option</b>	<b>Description</b>		
	<i>emergency</i>	Emergency level.		
	<i>alert</i>	Alert level.		
	<i>critical</i>	Critical level.		
	<i>error</i>	Error level.		
	<i>warning</i>	Warning level.		
	<i>notification</i>	Notification level.		
	<i>information</i>	Information level.		
	<i>debug</i>	Debug level.		
sta-locate-log	Lowest severity level to log station locate message.	option	-	notification
	<b>Option</b>	<b>Description</b>		
	<i>emergency</i>	Emergency level.		
	<i>alert</i>	Alert level.		
	<i>critical</i>	Critical level.		
	<i>error</i>	Error level.		
	<i>warning</i>	Warning level.		
	<i>notification</i>	Notification level.		

Parameter	Description	Type	Size	Default																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>information</i></td><td>Information level.</td></tr><tr><td><i>debug</i></td><td>Debug level.</td></tr></table>	Option	Description	<i>information</i>	Information level.	<i>debug</i>	Debug level.															
	Option	Description																				
	<i>information</i>	Information level.																				
<i>debug</i>	Debug level.																					
status	Enable/disable wireless event logging.	option	-	enable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable wireless event logging.</td></tr><tr><td><i>disable</i></td><td>Disable wireless event logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable wireless event logging.	<i>disable</i>	Disable wireless event logging.															
	Option	Description																				
	<i>enable</i>	Enable wireless event logging.																				
<i>disable</i>	Disable wireless event logging.																					
wids-log	Lowest severity level to log WIDS message.	option	-	notification																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>emergency</i></td><td>Emergency level.</td></tr><tr><td><i>alert</i></td><td>Alert level.</td></tr><tr><td><i>critical</i></td><td>Critical level.</td></tr><tr><td><i>error</i></td><td>Error level.</td></tr><tr><td><i>warning</i></td><td>Warning level.</td></tr><tr><td><i>notification</i></td><td>Notification level.</td></tr><tr><td><i>information</i></td><td>Information level.</td></tr><tr><td><i>debug</i></td><td>Debug level.</td></tr></table>	Option	Description	<i>emergency</i>	Emergency level.	<i>alert</i>	Alert level.	<i>critical</i>	Critical level.	<i>error</i>	Error level.	<i>warning</i>	Warning level.	<i>notification</i>	Notification level.	<i>information</i>	Information level.	<i>debug</i>	Debug level.			
	Option	Description																				
	<i>emergency</i>	Emergency level.																				
	<i>alert</i>	Alert level.																				
	<i>critical</i>	Critical level.																				
	<i>error</i>	Error level.																				
	<i>warning</i>	Warning level.																				
	<i>notification</i>	Notification level.																				
	<i>information</i>	Information level.																				
<i>debug</i>	Debug level.																					
wtp-event-log	Lowest severity level to log WTP event message.	option	-	notification																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>emergency</i></td><td>Emergency level.</td></tr><tr><td><i>alert</i></td><td>Alert level.</td></tr><tr><td><i>critical</i></td><td>Critical level.</td></tr><tr><td><i>error</i></td><td>Error level.</td></tr><tr><td><i>warning</i></td><td>Warning level.</td></tr><tr><td><i>notification</i></td><td>Notification level.</td></tr><tr><td><i>information</i></td><td>Information level.</td></tr><tr><td><i>debug</i></td><td>Debug level.</td></tr></table>	Option	Description	<i>emergency</i>	Emergency level.	<i>alert</i>	Alert level.	<i>critical</i>	Critical level.	<i>error</i>	Error level.	<i>warning</i>	Warning level.	<i>notification</i>	Notification level.	<i>information</i>	Information level.	<i>debug</i>	Debug level.			
	Option	Description																				
	<i>emergency</i>	Emergency level.																				
	<i>alert</i>	Alert level.																				
	<i>critical</i>	Critical level.																				
	<i>error</i>	Error level.																				
	<i>warning</i>	Warning level.																				
	<i>notification</i>	Notification level.																				
<i>information</i>	Information level.																					
<i>debug</i>	Debug level.																					

## config wireless-controller mpsk-profile

Configure MPSK profile.

```

config wireless-controller mpsk-profile
  Description: Configure MPSK profile.
  edit <name>
    set mpsk-concurrent-clients {integer}
  config mpsk-group
    Description: List of multiple PSK groups.
    edit <name>
      set vlan-type [no-vlan|fixed-vlan]
      set vlan-id {integer}
      config mpsk-key
        Description: List of multiple PSK entries.
        edit <name>
          set mac {mac-address}
          set passphrase {password}
          set concurrent-client-limit-type [default|unlimited|...]
          set concurrent-clients {integer}
          set comment {var-string}
          set mpsk-schedules <name1>, <name2>, ...
        next
      end
    next
  end
next
end

```

## config wireless-controller mpsk-profile

Parameter	Description	Type	Size	Default
mps-k-concurrent-clients	Maximum number of concurrent clients that connect using the same passphrase in multiple PSK authentication.	integer	Minimum value: 0 Maximum value: 65535	0
name	MPSK profile name.	string	Maximum length: 35	

## config mpsk-group

Parameter	Description	Type	Size	Default
name	MPSK group name.	string	Maximum length: 35	
vlan-type	MPSK group VLAN options.	option	-	no-vlan
	Option	Description		
	no-vlan	No VLAN.		
	fixed-vlan	Fixed VLAN ID.		

Parameter	Description	Type	Size	Default
vlan-id	Optional VLAN ID.	integer	Minimum value: 1 Maximum value: 4094	0

### config mpsk-key

Parameter	Description	Type	Size	Default								
name	Pre-shared key name.	string	Maximum length: 35									
mac	MAC address.	mac-address	Not Specified	00:00:00:00:00:00								
passphrase	WPA Pre-shared key.	password	Not Specified									
concurrent-client-limit-type	MPSK client limit type options.	option	-	default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>default</i></td><td>Using the value in profile configuration.</td></tr><tr><td><i>unlimited</i></td><td>Unlimited.</td></tr><tr><td><i>specified</i></td><td>Specified value.</td></tr></table>				Option	Description	<i>default</i>	Using the value in profile configuration.	<i>unlimited</i>	Unlimited.	<i>specified</i>	Specified value.
Option	Description											
<i>default</i>	Using the value in profile configuration.											
<i>unlimited</i>	Unlimited.											
<i>specified</i>	Specified value.											
concurrent-clients	Number of clients that can connect using this pre-shared key.	integer	Minimum value: 1 Maximum value: 65535	256								
comment	Comment.	var-string	Maximum length: 255									
mpsk-schedules <name>	Firewall schedule for MPSK passphrase. The passphrase will be effective only when at least one schedule is valid. Schedule name.	string	Maximum length: 35									

## config wireless-controller nac-profile

Configure WiFi network access control (NAC) profiles.

```
config wireless-controller nac-profile
    Description: Configure WiFi network access control (NAC) profiles.
    edit <name>
```

```

        set comment {var-string}
        set onboarding-vlan {string}
    next
end

```

## config wireless-controller nac-profile

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 255	
name	Name.	string	Maximum length: 35	
onboarding-vlan	VLAN interface name.	string	Maximum length: 35	

## config wireless-controller qos-profile

Configure WiFi quality of service (QoS) profiles.

```

config wireless-controller qos-profile
    Description: Configure WiFi quality of service (QoS) profiles.
    edit <name>
        set bandwidth-admission-control [enable|disable]
        set bandwidth-capacity {integer}
        set burst [enable|disable]
        set call-admission-control [enable|disable]
        set call-capacity {integer}
        set comment {string}
        set downlink {integer}
        set downlink-sta {integer}
        set dscp-wmm-be <id1>, <id2>, ...
        set dscp-wmm-bk <id1>, <id2>, ...
        set dscp-wmm-mapping [enable|disable]
        set dscp-wmm-vi <id1>, <id2>, ...
        set dscp-wmm-vo <id1>, <id2>, ...
        set uplink {integer}
        set uplink-sta {integer}
        set wmm [enable|disable]
        set wmm-be-dscp {integer}
        set wmm-bk-dscp {integer}
        set wmm-dscp-marking [enable|disable]
        set wmm-uapsd [enable|disable]
        set wmm-vi-dscp {integer}
        set wmm-vo-dscp {integer}
    next
end

```

## config wireless-controller qos-profile

Parameter	Description	Type	Size	Default						
bandwidth-admission-control	Enable/disable WMM bandwidth admission control.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable WMM bandwidth admission control.</td></tr><tr><td><i>disable</i></td><td>Disable WMM bandwidth admission control.</td></tr></table>	Option	Description	<i>enable</i>	Enable WMM bandwidth admission control.	<i>disable</i>	Disable WMM bandwidth admission control.			
Option	Description									
<i>enable</i>	Enable WMM bandwidth admission control.									
<i>disable</i>	Disable WMM bandwidth admission control.									
bandwidth-capacity	Maximum bandwidth capacity allowed.	integer	Minimum value: 1 Maximum value: 600000	2000						
burst	Enable/disable client rate burst.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable client rate burst.</td></tr><tr><td><i>disable</i></td><td>Disable client rate burst.</td></tr></table>	Option	Description	<i>enable</i>	Enable client rate burst.	<i>disable</i>	Disable client rate burst.			
Option	Description									
<i>enable</i>	Enable client rate burst.									
<i>disable</i>	Disable client rate burst.									
call-admission-control	Enable/disable WMM call admission control.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable WMM call admission control.</td></tr><tr><td><i>disable</i></td><td>Disable WMM call admission control.</td></tr></table>	Option	Description	<i>enable</i>	Enable WMM call admission control.	<i>disable</i>	Disable WMM call admission control.			
Option	Description									
<i>enable</i>	Enable WMM call admission control.									
<i>disable</i>	Disable WMM call admission control.									
call-capacity	Maximum number of Voice over WLAN.	integer	Minimum value: 0 Maximum value: 60	10						
comment	Comment.	string	Maximum length: 63							
downlink	Maximum downlink bandwidth for Virtual Access Points.	integer	Minimum value: 0 Maximum value: 2097152	0						

Parameter	Description	Type	Size	Default						
downlink-sta	Maximum downlink bandwidth for clients.	integer	Minimum value: 0 Maximum value: 2097152	0						
dscp-wmm-be<id>	DSCP mapping for best effort access (default = 0 24). DSCP WMM mapping numbers (0 - 63).	integer	Minimum value: 0 Maximum value: 63							
dscp-wmm-bk<id>	DSCP mapping for background access (default = 8 16). DSCP WMM mapping numbers (0 - 63).	integer	Minimum value: 0 Maximum value: 63							
dscp-wmm-mapping	Enable/disable Differentiated Services Code Point (DSCP) mapping.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable Differentiated Services Code Point (DSCP) mapping.</td></tr><tr><td>disable</td><td>Disable Differentiated Services Code Point (DSCP) mapping.</td></tr></table>				Option	Description	enable	Enable Differentiated Services Code Point (DSCP) mapping.	disable	Disable Differentiated Services Code Point (DSCP) mapping.
Option	Description									
enable	Enable Differentiated Services Code Point (DSCP) mapping.									
disable	Disable Differentiated Services Code Point (DSCP) mapping.									
dscp-wmm-vi<id>	DSCP mapping for video access (default = 32 40). DSCP WMM mapping numbers (0 - 63).	integer	Minimum value: 0 Maximum value: 63							
dscp-wmm-vo<id>	DSCP mapping for voice access (default = 48 56). DSCP WMM mapping numbers (0 - 63).	integer	Minimum value: 0 Maximum value: 63							
name	WiFi QoS profile name.	string	Maximum length: 35							
uplink	Maximum uplink bandwidth for Virtual Access Points.	integer	Minimum value: 0 Maximum value: 2097152	0						
uplink-sta	Maximum uplink bandwidth for clients.	integer	Minimum value: 0 Maximum value: 2097152	0						
wmm	Enable/disable WiFi multi-media (WMM) control.	option	-	enable						

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable WiFi multi-media (WMM) control.		
	<i>disable</i>	Disable WiFi multi-media (WMM) control.		
wmm-be-dscp	DSCP marking for best effort access.	integer	Minimum value: 0 Maximum value: 63	0
wmm-bk-dscp	DSCP marking for background access.	integer	Minimum value: 0 Maximum value: 63	8
wmm-dscp-marking	Enable/disable WMM Differentiated Services Code Point (DSCP) marking.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable WMM Differentiated Services Code Point (DSCP) marking.		
	<i>disable</i>	Disable WMM Differentiated Services Code Point (DSCP) marking.		
wmm-uapsd	Enable/disable WMM Unscheduled Automatic Power Save Delivery (U-APSD) power save mode.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable WMM Unscheduled Automatic Power Save Delivery (U-APSD) power save mode.		
	<i>disable</i>	Disable WMM Unscheduled Automatic Power Save Delivery (U-APSD) power save mode.		
wmm-vi-dscp	DSCP marking for video access.	integer	Minimum value: 0 Maximum value: 63	32
wmm-vo-dscp	DSCP marking for voice access.	integer	Minimum value: 0 Maximum value: 63	48

## config wireless-controller region

Configure FortiAP regions (for floor plans and maps).

```
config wireless-controller region
    Description: Configure FortiAP regions (for floor plans and maps).
```



```

edit <name>
    set comments {string}
    set grayscale [enable|disable]
    set opacity {integer}
next
end

```

## config wireless-controller region

Parameter	Description	Type	Size	Default						
comments	Comments.	string	Maximum length: 1027							
grayscale	Region image grayscale.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable region image grayscale.</td></tr><tr><td><i>disable</i></td><td>Disable region image grayscale.</td></tr></table>				Option	Description	<i>enable</i>	Enable region image grayscale.	<i>disable</i>	Disable region image grayscale.
	Option	Description								
	<i>enable</i>	Enable region image grayscale.								
<i>disable</i>	Disable region image grayscale.									
name	FortiAP region name.	string	Maximum length: 35							
opacity	Region image opacity.	integer	Minimum value: 0 Maximum value: 100	100						

## config wireless-controller setting

VDOM wireless controller configuration.

```

config wireless-controller setting
    Description: VDOM wireless controller configuration.
    set account-id {string}
    set country [--|AF|...]
    set darrp-optimize {integer}
    set darrp-optimize-schedules <name1>, <name2>, ...
    set device-holdoff {integer}
    set device-idle {integer}
    set device-weight {integer}
    set duplicate-ssid [enable|disable]
    set fake-ssid-action {option1}, {option2}, ...
    set fapc-compatibility [enable|disable]
    set firmware-provision-on-authorization [enable|disable]
    config offending-ssid
        Description: Configure offending SSID.
        edit <id>
            set ssid-pattern {string}
            set action {option1}, {option2}, ...
        next
    end
end

```

```

end
set phishing-ssid-detect [enable|disable]
set wfa-compatibility [enable|disable]
end

```

## config wireless-controller setting

Parameter	Description	Type	Size	Default
account-id	FortiCloud customer account ID.	string	Maximum length: 63	
country	Country or region in which the FortiGate is located. The country determines the 802.11 bands and channels that are available.	option	-	US

Option	Description
--	NO_COUNTRY_SET
AF	AFGHANISTAN
AL	ALBANIA
DZ	ALGERIA
AS	AMERICAN SAMOA
AO	ANGOLA
AR	ARGENTINA
AM	ARMENIA
AU	AUSTRALIA
AT	AUSTRIA
AZ	AZERBAIJAN
BS	BAHAMAS
BH	BAHRAIN
BD	BANGLADESH
BB	BARBADOS
BY	BELARUS
BE	BELGIUM
BZ	BELIZE
BJ	BENIN
BM	BERMUDA

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>BT</i>	BHUTAN		
	<i>BO</i>	BOLIVIA		
	<i>BA</i>	BOSNIA AND HERZEGOVINA		
	<i>BW</i>	BOTSWANA		
	<i>BR</i>	BRAZIL		
	<i>BN</i>	BRUNEI DARUSSALAM		
	<i>BG</i>	BULGARIA		
	<i>BF</i>	BURKINA-FASO		
	<i>KH</i>	CAMBODIA		
	<i>CM</i>	CAMEROON		
	<i>KY</i>	CAYMAN ISLANDS		
	<i>CF</i>	CENTRAL AFRICA REPUBLIC		
	<i>TD</i>	CHAD		
	<i>CL</i>	CHILE		
	<i>CN</i>	CHINA		
	<i>CX</i>	CHRISTMAS ISLAND		
	<i>CO</i>	COLOMBIA		
	<i>CG</i>	CONGO REPUBLIC		
	<i>CD</i>	DEMOCRATIC REPUBLIC OF CONGO		
	<i>CR</i>	COSTA RICA		
	<i>HR</i>	CROATIA		
	<i>CY</i>	CYPRUS		
	<i>CZ</i>	CZECH REPUBLIC		
	<i>DK</i>	DENMARK		
	<i>DM</i>	DOMINICA		
	<i>DO</i>	DOMINICAN REPUBLIC		
	<i>EC</i>	ECUADOR		
	<i>EG</i>	EGYPT		
	<i>SV</i>	EL SALVADOR		

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>ET</i>	ETHIOPIA		
	<i>EE</i>	ESTONIA		
	<i>GF</i>	FRENCH GUIANA		
	<i>PF</i>	FRENCH POLYNESIA		
	<i>FO</i>	FAEROE ISLANDS		
	<i>FJ</i>	FIJI		
	<i>FI</i>	FINLAND		
	<i>FR</i>	FRANCE		
	<i>GE</i>	GEORGIA		
	<i>DE</i>	GERMANY		
	<i>GH</i>	GHANA		
	<i>GI</i>	GIBRALTAR		
	<i>GR</i>	GREECE		
	<i>GL</i>	GREENLAND		
	<i>GD</i>	GRENADA		
	<i>GP</i>	GUADELOUPE		
	<i>GU</i>	GUAM		
	<i>GT</i>	GUATEMALA		
	<i>GY</i>	GUYANA		
	<i>HT</i>	HAITI		
	<i>HN</i>	HONDURAS		
	<i>HK</i>	HONG KONG		
	<i>HU</i>	HUNGARY		
	<i>IS</i>	ICELAND		
	<i>IN</i>	INDIA		
	<i>ID</i>	INDONESIA		
	<i>IQ</i>	IRAQ		
	<i>IE</i>	IRELAND		
	<i>IM</i>	ISLE OF MAN		

Parameter	Description	Type	Size	Default
-----------	-------------	------	------	---------

Option	Description
<i>IL</i>	ISRAEL
<i>IT</i>	ITALY
<i>CI</i>	COTE_D_IVOIRE
<i>JM</i>	JAMAICA
<i>JO</i>	JORDAN
<i>KZ</i>	KAZAKHSTAN
<i>KE</i>	KENYA
<i>KR</i>	KOREA REPUBLIC
<i>KW</i>	KUWAIT
<i>LA</i>	LAOS
<i>LV</i>	LATVIA
<i>LB</i>	LEBANON
<i>LS</i>	LESOTHO
<i>LY</i>	LIBYA
<i>LI</i>	LIECHTENSTEIN
<i>LT</i>	LITHUANIA
<i>LU</i>	LUXEMBOURG
<i>MO</i>	MACAU SAR
<i>MK</i>	MACEDONIA, FYRO
<i>MG</i>	MADAGASCAR
<i>MW</i>	MALAWI
<i>MY</i>	MALAYSIA
<i>MV</i>	MALDIVES
<i>ML</i>	MALI
<i>MT</i>	MALTA
<i>MH</i>	MARSHALL ISLANDS
<i>MQ</i>	MARTINIQUE
<i>MR</i>	MAURITANIA
<i>MU</i>	MAURITIUS

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>YT</i>	MAYOTTE		
	<i>MX</i>	MEXICO		
	<i>FM</i>	MICRONESIA		
	<i>MD</i>	REPUBLIC OF MOLDOVA		
	<i>MC</i>	MONACO		
	<i>MN</i>	MONGOLIA		
	<i>MA</i>	MOROCCO		
	<i>MZ</i>	MOZAMBIQUE		
	<i>MM</i>	MYANMAR		
	<i>NA</i>	NAMIBIA		
	<i>NP</i>	NEPAL		
	<i>NL</i>	NETHERLANDS		
	<i>AN</i>	NETHERLANDS ANTILLES		
	<i>AW</i>	ARUBA		
	<i>NZ</i>	NEW ZEALAND		
	<i>NI</i>	NICARAGUA		
	<i>NE</i>	NIGER		
	<i>NO</i>	NORWAY		
	<i>MP</i>	NORTHERN MARIANA ISLANDS		
	<i>OM</i>	OMAN		
	<i>PK</i>	PAKISTAN		
	<i>PW</i>	PALAU		
	<i>PA</i>	PANAMA		
	<i>PG</i>	PAPUA NEW GUINEA		
	<i>PY</i>	PARAGUAY		
	<i>PE</i>	PERU		
	<i>PH</i>	PHILIPPINES		
	<i>PL</i>	POLAND		
	<i>PT</i>	PORTUGAL		

Parameter	Description	Type	Size	Default
-----------	-------------	------	------	---------

Option	Description
<i>PR</i>	PUERTO RICO
<i>QA</i>	QATAR
<i>RE</i>	REUNION
<i>RO</i>	ROMANIA
<i>RU</i>	RUSSIA
<i>RW</i>	RWANDA
<i>BL</i>	SAINT BARTHELEMY
<i>KN</i>	SAINT KITTS AND NEVIS
<i>LC</i>	SAINT LUCIA
<i>MF</i>	SAINT MARTIN
<i>PM</i>	SAINT PIERRE AND MIQUELON
<i>VC</i>	SAINT VINCENT AND GRENADIENS
<i>SA</i>	SAUDI ARABIA
<i>SN</i>	SENEGAL
<i>RS</i>	REPUBLIC OF SERBIA
<i>ME</i>	MONTENEGRO
<i>SL</i>	SIERRA LEONE
<i>SG</i>	SINGAPORE
<i>SK</i>	SLOVAKIA
<i>SI</i>	SLOVENIA
<i>ZA</i>	SOUTH AFRICA
<i>ES</i>	SPAIN
<i>LK</i>	SRI LANKA
<i>SE</i>	SWEDEN
<i>SR</i>	SURINAME
<i>CH</i>	SWITZERLAND
<i>TW</i>	TAIWAN
<i>TZ</i>	TANZANIA
<i>TH</i>	THAILAND

Parameter	Description	Type	Size	Default																																																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>TG</td><td>TOGO</td></tr><tr><td>TT</td><td>TRINIDAD AND TOBAGO</td></tr><tr><td>TN</td><td>TUNISIA</td></tr><tr><td>TR</td><td>TURKEY</td></tr><tr><td>TM</td><td>TURKMENISTAN</td></tr><tr><td>AE</td><td>UNITED ARAB EMIRATES</td></tr><tr><td>TC</td><td>TURKS AND CAICOS</td></tr><tr><td>UG</td><td>UGANDA</td></tr><tr><td>UA</td><td>UKRAINE</td></tr><tr><td>GB</td><td>UNITED KINGDOM</td></tr><tr><td>US</td><td>UNITED STATES2</td></tr><tr><td>PS</td><td>UNITED STATES (PUBLIC SAFETY)</td></tr><tr><td>UY</td><td>URUGUAY</td></tr><tr><td>UZ</td><td>UZBEKISTAN</td></tr><tr><td>VU</td><td>VANUATU</td></tr><tr><td>VE</td><td>VENEZUELA</td></tr><tr><td>VN</td><td>VIET NAM</td></tr><tr><td>VI</td><td>VIRGIN ISLANDS</td></tr><tr><td>WF</td><td>WALLIS AND FUTUNA</td></tr><tr><td>YE</td><td>YEMEN</td></tr><tr><td>ZM</td><td>ZAMBIA</td></tr><tr><td>ZW</td><td>ZIMBABWE</td></tr><tr><td>JP</td><td>JAPAN14</td></tr><tr><td>CA</td><td>CANADA2</td></tr></table>	Option	Description	TG	TOGO	TT	TRINIDAD AND TOBAGO	TN	TUNISIA	TR	TURKEY	TM	TURKMENISTAN	AE	UNITED ARAB EMIRATES	TC	TURKS AND CAICOS	UG	UGANDA	UA	UKRAINE	GB	UNITED KINGDOM	US	UNITED STATES2	PS	UNITED STATES (PUBLIC SAFETY)	UY	URUGUAY	UZ	UZBEKISTAN	VU	VANUATU	VE	VENEZUELA	VN	VIET NAM	VI	VIRGIN ISLANDS	WF	WALLIS AND FUTUNA	YE	YEMEN	ZM	ZAMBIA	ZW	ZIMBABWE	JP	JAPAN14	CA	CANADA2			
	Option	Description																																																				
	TG	TOGO																																																				
	TT	TRINIDAD AND TOBAGO																																																				
	TN	TUNISIA																																																				
	TR	TURKEY																																																				
	TM	TURKMENISTAN																																																				
	AE	UNITED ARAB EMIRATES																																																				
	TC	TURKS AND CAICOS																																																				
	UG	UGANDA																																																				
	UA	UKRAINE																																																				
	GB	UNITED KINGDOM																																																				
	US	UNITED STATES2																																																				
	PS	UNITED STATES (PUBLIC SAFETY)																																																				
	UY	URUGUAY																																																				
	UZ	UZBEKISTAN																																																				
	VU	VANUATU																																																				
	VE	VENEZUELA																																																				
	VN	VIET NAM																																																				
	VI	VIRGIN ISLANDS																																																				
	WF	WALLIS AND FUTUNA																																																				
	YE	YEMEN																																																				
	ZM	ZAMBIA																																																				
	ZW	ZIMBABWE																																																				
	JP	JAPAN14																																																				
	CA	CANADA2																																																				
darrp-optimize	Time for running Dynamic Automatic Radio Resource Provisioning.	integer	Minimum value: 0 Maximum value: 86400	86400																																																		



Parameter	Description	Type	Size	Default						
darrp-optimize-schedules <name>	Firewall schedules for DARRP running time. DARRP will run periodically based on darrp-optimize within the schedules. Separate multiple schedule names with a space. Schedule name.	string	Maximum length: 35							
device-holdoff	Lower limit of creation time of device for identification in minutes.	integer	Minimum value: 0 Maximum value: 60	5						
device-idle	Upper limit of idle time of device for identification in minutes.	integer	Minimum value: 0 Maximum value: 14400	1440						
device-weight	Upper limit of confidence of device for identification.	integer	Minimum value: 0 Maximum value: 255	1						
duplicate-ssid	Enable/disable allowing Virtual Access Points (VAPs) to use the same SSID name in the same VDOM.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Allow VAPs to use the same SSID name in the same VDOM.</td></tr><tr><td>disable</td><td>Do not allow VAPs to use the same SSID name in the same VDOM.</td></tr></table>				Option	Description	enable	Allow VAPs to use the same SSID name in the same VDOM.	disable	Do not allow VAPs to use the same SSID name in the same VDOM.
Option	Description									
enable	Allow VAPs to use the same SSID name in the same VDOM.									
disable	Do not allow VAPs to use the same SSID name in the same VDOM.									
fake-ssid-action	Actions taken for detected fake SSID.	option	-	log						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>log</td><td>Write logs for detected fake SSID.</td></tr><tr><td>suppress</td><td>Suppress detected fake SSID.</td></tr></table>				Option	Description	log	Write logs for detected fake SSID.	suppress	Suppress detected fake SSID.
Option	Description									
log	Write logs for detected fake SSID.									
suppress	Suppress detected fake SSID.									
fapc-compatibility	Enable/disable FAP-C series compatibility.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable FAP-C series compatibility.</td></tr><tr><td>disable</td><td>Disable FAP-C series compatibility.</td></tr></table>				Option	Description	enable	Enable FAP-C series compatibility.	disable	Disable FAP-C series compatibility.
Option	Description									
enable	Enable FAP-C series compatibility.									
disable	Disable FAP-C series compatibility.									

Parameter	Description	Type	Size	Default						
firmware-provision-on-authorization	Enable/disable automatic provisioning of latest firmware on authorization.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable firmware provision on authorization.</td></tr><tr><td><i>disable</i></td><td>Disable firmware provision on authorization.</td></tr></table>	Option	Description	<i>enable</i>	Enable firmware provision on authorization.	<i>disable</i>	Disable firmware provision on authorization.			
Option	Description									
<i>enable</i>	Enable firmware provision on authorization.									
<i>disable</i>	Disable firmware provision on authorization.									
phishing-ssid-detect	Enable/disable phishing SSID detection.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable phishing SSID detection.</td></tr><tr><td><i>disable</i></td><td>Disable phishing SSID detection.</td></tr></table>	Option	Description	<i>enable</i>	Enable phishing SSID detection.	<i>disable</i>	Disable phishing SSID detection.			
Option	Description									
<i>enable</i>	Enable phishing SSID detection.									
<i>disable</i>	Disable phishing SSID detection.									
wfa-compatibility	Enable/disable WFA compatibility.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Wi-Fi Alliance Certification compatibility.</td></tr><tr><td><i>disable</i></td><td>Disable Wi-Fi Alliance Certification compatibility.</td></tr></table>	Option	Description	<i>enable</i>	Enable Wi-Fi Alliance Certification compatibility.	<i>disable</i>	Disable Wi-Fi Alliance Certification compatibility.			
Option	Description									
<i>enable</i>	Enable Wi-Fi Alliance Certification compatibility.									
<i>disable</i>	Disable Wi-Fi Alliance Certification compatibility.									

### config offending-ssid

Parameter	Description	Type	Size	Default						
id	ID.	integer	Minimum value: 0 Maximum value: 65535	0						
ssid-pattern	Define offending SSID pattern (case insensitive). For example, word, word*, *word, wo*rd.	string	Maximum length: 33							
action	Actions taken for detected offending SSID.	option	-	log						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>log</td><td>Generate logs for detected offending SSID.</td></tr><tr><td>suppress</td><td>Suppress detected offending SSID.</td></tr></table>				Option	Description	log	Generate logs for detected offending SSID.	suppress	Suppress detected offending SSID.
Option	Description									
log	Generate logs for detected offending SSID.									
suppress	Suppress detected offending SSID.									

### config wireless-controller snmp

Configure SNMP.

```

config wireless-controller snmp
  Description: Configure SNMP.
  config community
    Description: SNMP Community Configuration.
    edit <id>
      set name {string}
      set status [enable|disable]
      set query-v1-status [enable|disable]
      set query-v2c-status [enable|disable]
      set trap-v1-status [enable|disable]
      set trap-v2c-status [enable|disable]
      config hosts
        Description: Configure IPv4 SNMP managers (hosts).
        edit <id>
          set ip {user}
        next
      end
    next
  end
  set contact-info {string}
  set engine-id {string}
  set trap-high-cpu-threshold {integer}
  set trap-high-mem-threshold {integer}
  config user
    Description: SNMP User Configuration.
    edit <name>
      set status [enable|disable]
      set queries [enable|disable]
      set trap-status [enable|disable]
      set security-level [no-auth-no-priv|auth-no-priv|...]
      set auth-proto [md5|sha]
      set auth-pwd {password}
      set priv-proto [aes|des|...]
      set priv-pwd {password}
      set notify-hosts {ipv4-address}
    next
  end
end

```

## config wireless-controller snmp

Parameter	Description	Type	Size	Default
contact-info	Contact Information.	string	Maximum length: 31	
engine-id	AC SNMP engineID string (maximum 24 characters).	string	Maximum length: 23	
trap-high-cpu-threshold	CPU usage when trap is sent.	integer	Minimum value: 10 Maximum value: 100	80

Parameter	Description	Type	Size	Default
trap-high-mem-threshold	Memory usage when trap is sent.	integer	Minimum value: 10 Maximum value: 100	80

## config community

Parameter	Description	Type	Size	Default						
id	Community ID.	integer	Minimum value: 0 Maximum value: 4294967295	0						
name	Community name.	string	Maximum length: 35							
status	Enable/disable this SNMP community.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
query-v1-status	Enable/disable SNMP v1 queries.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
query-v2c-status	Enable/disable SNMP v2c queries.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
trap-v1-status	Enable/disable SNMP v1 traps.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									

Parameter	Description	Type	Size	Default
trap-v2c-status	Enable/disable SNMP v2c traps.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

## config hosts

Parameter	Description	Type	Size	Default
id	Host entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
ip	IPv4 address of the SNMP manager (host).	user	Not Specified	

## config user

Parameter	Description	Type	Size	Default
name	SNMP user name.	string	Maximum length: 32	test
status	SNMP user enable.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
queries	Enable/disable SNMP queries for this user.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		
trap-status	Enable/disable traps for this SNMP user.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable setting.		
	<i>disable</i>	Disable setting.		

Parameter	Description	Type	Size	Default
security-level	Security level for message authentication and encryption.	option	-	no-auth-no-priv
	<b>Option</b>	<b>Description</b>		
	<i>no-auth-no-priv</i>	Message with no authentication and no privacy (encryption).		
	<i>auth-no-priv</i>	Message with authentication but no privacy (encryption).		
	<i>auth-priv</i>	Message with authentication and privacy (encryption).		
auth-proto	Authentication protocol.	option	-	sha
	<b>Option</b>	<b>Description</b>		
	<i>md5</i>	HMAC-MD5-96 authentication protocol.		
	<i>sha</i>	HMAC-SHA-96 authentication protocol.		
auth-pwd	Password for authentication protocol.	password	Not Specified	
priv-proto	Privacy (encryption) protocol.	option	-	aes
	<b>Option</b>	<b>Description</b>		
	<i>aes</i>	CFB128-AES-128 symmetric encryption protocol.		
	<i>des</i>	CBC-DES symmetric encryption protocol.		
	<i>aes256</i>	CFB128-AES-256 symmetric encryption protocol.		
	<i>aes256cisco</i>	CFB128-AES-256 symmetric encryption protocol compatible with CISCO.		
priv-pwd	Password for privacy (encryption) protocol.	password	Not Specified	
notify-hosts	Configure SNMP User Notify Hosts.	ipv4-address	Not Specified	

## config wireless-controller ssid-policy

Configure WiFi SSID policies.

```

config wireless-controller ssid-policy
    Description: Configure WiFi SSID policies.
    edit <name>
        set description {var-string}
        set vlan {string}
    next
end

```

## config wireless-controller ssid-policy

Parameter	Description	Type	Size	Default
description	Description.	var-string	Maximum length: 255	
name	Name.	string	Maximum length: 35	
vlan	VLAN interface name.	string	Maximum length: 35	

## config wireless-controller syslog-profile

Configure Wireless Termination Points (WTP) system log server profile.

```
config wireless-controller syslog-profile
  Description: Configure Wireless Termination Points (WTP) system log server profile.
  edit <name>
    set comment {var-string}
    set log-level [emergency|alert|...]
    set server-addr-type [fqdn|ip]
    set server-fqdn {string}
    set server-ip {ipv4-address}
    set server-port {integer}
    set server-status [enable|disable]
  next
end
```

## config wireless-controller syslog-profile

Parameter	Description	Type	Size	Default														
comment	Comment.	var-string	Maximum length: 255															
log-level	Lowest level of log messages that FortiAP units send to this server.	option	-	information														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>emergency</i></td><td>Level 0</td></tr><tr><td><i>alert</i></td><td>Level 1</td></tr><tr><td><i>critical</i></td><td>Level 2</td></tr><tr><td><i>error</i></td><td>Level 3</td></tr><tr><td><i>warning</i></td><td>Level 4</td></tr><tr><td><i>notification</i></td><td>Level 5</td></tr></table>				Option	Description	<i>emergency</i>	Level 0	<i>alert</i>	Level 1	<i>critical</i>	Level 2	<i>error</i>	Level 3	<i>warning</i>	Level 4	<i>notification</i>	Level 5
	Option	Description																
	<i>emergency</i>	Level 0																
	<i>alert</i>	Level 1																
	<i>critical</i>	Level 2																
	<i>error</i>	Level 3																
	<i>warning</i>	Level 4																
<i>notification</i>	Level 5																	

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>information</i>	Level 6		
	<i>debugging</i>	Level 7		
name	WTP system log server profile name.	string	Maximum length: 35	
server-addr-type	Syslog server address type.	option	-	ip
	<b>Option</b>	<b>Description</b>		
	<i>fqdn</i>	Fully Qualified Domain Name address.		
	<i>ip</i>	IPv4 address.		
server-fqdn	FQDN of syslog server that FortiAP units send log messages to.	string	Maximum length: 63	
server-ip	IP address of syslog server that FortiAP units send log messages to.	ipv4-address	Not Specified	0.0.0.0
server-port	Port number of syslog server that FortiAP units send log messages to.	integer	Minimum value: 0 Maximum value: 65535	514
server-status	Enable/disable FortiAP units to send log messages to a syslog server.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable syslog server.		
	<i>disable</i>	Disable syslog server.		

## config wireless-controller timers

Configure CAPWAP timers.

```
config wireless-controller timers
  Description: Configure CAPWAP timers.
  set auth-timeout {integer}
  set ble-scan-report-intv {integer}
  set client-idle-timeout {integer}
  set discovery-interval {integer}
  set drma-interval {integer}
  set echo-interval {integer}
  set fake-ap-log {integer}
  set ipsec-intf-cleanup {integer}
```



```

set radio-stats-interval {integer}
set rogue-ap-cleanup {integer}
set rogue-ap-log {integer}
set sta-capability-interval {integer}
set sta-locate-timer {integer}
set sta-stats-interval {integer}
set vap-stats-interval {integer}
end

```

## config wireless-controller timers

Parameter	Description	Type	Size	Default
auth-timeout	Time after which a client is considered failed in RADIUS authentication and times out.	integer	Minimum value: 5 Maximum value: 30	5
ble-scan-report-intv	Time between running Bluetooth Low Energy.	integer	Minimum value: 10 Maximum value: 3600	30
client-idle-timeout	Time after which a client is considered idle and times out.	integer	Minimum value: 20 Maximum value: 3600	300
discovery-interval	Time between discovery requests.	integer	Minimum value: 2 Maximum value: 180	5
drma-interval	Dynamic radio mode assignment.	integer	Minimum value: 1 Maximum value: 1440	60
echo-interval	Time between echo requests sent by the managed WTP, AP, or FortiAP.	integer	Minimum value: 1 Maximum value: 255	30
fake-ap-log	Time between recording logs about fake APs if periodic fake AP logging is configured.	integer	Minimum value: 1 Maximum value: 1440	1
ipsec-intf-cleanup	Time period to keep IPsec VPN interfaces up after WTP sessions are disconnected.	integer	Minimum value: 30 Maximum value: 3600	120

Parameter	Description	Type	Size	Default
radio-stats-interval	Time between running radio reports.	integer	Minimum value: 1 Maximum value: 255	15
rogue-ap-cleanup	Time period in minutes to keep rogue AP after it is gone.	integer	Minimum value: 0 Maximum value: 4294967295	0
rogue-ap-log	Time between logging rogue AP messages if periodic rogue AP logging is configured.	integer	Minimum value: 0 Maximum value: 1440	0
sta-capability-interval	Time between running station capability reports.	integer	Minimum value: 1 Maximum value: 255	30
sta-locate-timer	Time between running client presence flushes to remove clients that are listed but no longer present.	integer	Minimum value: 0 Maximum value: 86400	1800
sta-stats-interval	Time between running client.	integer	Minimum value: 1 Maximum value: 255	1
vap-stats-interval	Time between running Virtual Access Point.	integer	Minimum value: 1 Maximum value: 255	15

## config wireless-controller vap-group

Configure virtual Access Point (VAP) groups.

```

config wireless-controller vap-group
    Description: Configure virtual Access Point (VAP) groups.
    edit <name>
        set comment {var-string}
        set vaps <name1>, <name2>, ...
    next
end

```

## config wireless-controller vap-group

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 255	
name	Group Name.	string	Maximum length: 35	
vaps <name>	List of SSIDs to be included in the VAP group. VAP name.	string	Maximum length: 35	

## config wireless-controller vap

Configure Virtual Access Points (VAPs).

```
config wireless-controller vap
  Description: Configure Virtual Access Points (VAPs).
  edit <name>
    set access-control-list {string}
    set additional-akms {option1}, {option2}, ...
    set address-group {string}
    set antivirus-profile {string}
    set application-list {string}
    set atf-weight {integer}
    set auth [psk|radius|...]
    set auth-cert {string}
    set auth-portal-addr {string}
    set beacon-advertising {option1}, {option2}, ...
    set broadcast-ssid [enable|disable]
    set broadcast-suppression {option1}, {option2}, ...
    set bss-color-partial [enable|disable]
    set bstm-disassociation-imminent [enable|disable]
    set bstm-load-balancing-disassoc-timer {integer}
    set bstm-rssi-disassoc-timer {integer}
    set captive-portal-ac-name {string}
    set captive-portal-auth-timeout {integer}
    set dhcp-address-enforcement [enable|disable]
    set dhcp-lease-time {integer}
    set dhcp-option43-insertion [enable|disable]
    set dhcp-option82-circuit-id-insertion [style-1|style-2|...]
    set dhcp-option82-insertion [enable|disable]
    set dhcp-option82-remote-id-insertion [style-1|disable]
    set dynamic-vlan [enable|disable]
    set eap-reauth [enable|disable]
    set eap-reauth-intv {integer}
    set eapol-key-retries [disable|enable]
    set encrypt [TKIP|AES|...]
    set external-fast-roaming [enable|disable]
    set external-logout {string}
    set external-web {var-string}
    set external-web-format [auto-detect|no-query-string|...]
    set fast-bss-transition [disable|enable]
```

```

set fast-roaming [enable|disable]
set ft-mobility-domain {integer}
set ft-over-ds [disable|enable]
set ft-r0-key-lifetime {integer}
set gas-comeback-delay {integer}
set gas-fragmentation-limit {integer}
set gtk-rekey [enable|disable]
set gtk-rekey-intv {integer}
set high-efficiency [enable|disable]
set hotspot20-profile {string}
set igmp-snooping [enable|disable]
set intra-vap-privacy [enable|disable]
set ip {ipv4-classnet-host}
set ips-sensor {string}
set ipv6-rules {option1}, {option2}, ...
set key {password}
set keyindex {integer}
set ldpc [disable|rx|...]
set local-authentication [enable|disable]
set local-bridging [enable|disable]
set local-lan [allow|deny]
set local-standalone [enable|disable]
set local-standalone-dns [enable|disable]
set local-standalone-dns-ip {ipv4-address}
set local-standalone-nat [enable|disable]
set mac-auth-bypass [enable|disable]
set mac-called-station-delimiter [hyphen|single-hyphen|...]
set mac-calling-station-delimiter [hyphen|single-hyphen|...]
set mac-case [uppercase|lowercase]
set mac-filter [enable|disable]
config mac-filter-list
    Description: Create a list of MAC addresses for MAC address filtering.
    edit <id>
        set mac {mac-address}
        set mac-filter-policy [allow|deny]
    next
end
set mac-filter-policy-other [allow|deny]
set mac-password-delimiter [hyphen|single-hyphen|...]
set mac-username-delimiter [hyphen|single-hyphen|...]
set max-clients {integer}
set max-clients-ap {integer}
set mbo [disable|enable]
set mbo-cell-data-conn-pref [excluded|prefer-not|...]
set me-disable-thresh {integer}
set mesh-backhaul [enable|disable]
set mpsk-profile {string}
set mu-mimo [enable|disable]
set multicast-enhance [enable|disable]
set multicast-rate [0|6000|...]
set nac [enable|disable]
set nac-profile {string}
set neighbor-report-dual-band [disable|enable]
set okc [disable|enable]
set osen [enable|disable]
set owe-groups {option1}, {option2}, ...

```

```

set owe-transition [disable|enable]
set owe-transition-ssid {string}
set passphrase {password}
set pmf [disable|enable|...]
set pmf-assoc-comeback-timeout {integer}
set pmf-sa-query-retry-timeout {integer}
set port-macauth [disable|radius|...]
set port-macauth-reauth-timeout {integer}
set port-macauth-timeout {integer}
set portal-message-override-group {string}
config portal-message-overrides
    Description: Individual message overrides.
    set auth-disclaimer-page {string}
    set auth-reject-page {string}
    set auth-login-page {string}
    set auth-login-failed-page {string}
end
set portal-type [auth|auth+disclaimer|...]
set primary-wag-profile {string}
set probe-resp-suppression [enable|disable]
set probe-resp-threshold {string}
set ptk-rekey [enable|disable]
set ptk-rekey-intv {integer}
set qos-profile {string}
set quarantine [enable|disable]
set radio-2g-threshold {string}
set radio-5g-threshold {string}
set radio-sensitivity [enable|disable]
set radius-mac-auth [enable|disable]
set radius-mac-auth-server {string}
set radius-mac-auth-usergroups <name1>, <name2>, ...
set radius-mac-mpsk-auth [enable|disable]
set radius-mac-mpsk-timeout {integer}
set radius-server {string}
set rates-11a {option1}, {option2}, ...
set rates-11ac-ss12 {option1}, {option2}, ...
set rates-11ac-ss34 {option1}, {option2}, ...
set rates-11ax-ss12 {option1}, {option2}, ...
set rates-11ax-ss34 {option1}, {option2}, ...
set rates-11bg {option1}, {option2}, ...
set rates-11n-ss12 {option1}, {option2}, ...
set rates-11n-ss34 {option1}, {option2}, ...
set sae-groups {option1}, {option2}, ...
set sae-h2e-only [enable|disable]
set sae-password {password}
set sae-pk [enable|disable]
set sae-private-key {string}
set scan-botnet-connections [disable|monitor|...]
set schedule <name1>, <name2>, ...
set secondary-wag-profile {string}
set security [open|captive-portal|...]
set security-exempt-list {string}
set security-redirect-url {var-string}
set selected-usergroups <name1>, <name2>, ...
set split-tunneling [enable|disable]
set ssid {string}

```

```

set sticky-client-remove [enable|disable]
set sticky-client-threshold-2g {string}
set sticky-client-threshold-5g {string}
set sticky-client-threshold-6g {string}
set target-wake-time [enable|disable]
set tkip-counter-measure [enable|disable]
set tunnel-echo-interval {integer}
set tunnel-fallback-interval {integer}
set usergroup <name1>, <name2>, ...
set utm-log [enable|disable]
set utm-profile {string}
set utm-status [enable|disable]
set vlan-auto [enable|disable]
config vlan-name
    Description: Table for mapping VLAN name to VLAN ID.
    edit <name>
        set vlan-id {integer}
    next
end
config vlan-pool
    Description: VLAN pool.
    edit <id>
        set wtp-group {string}
    next
end
set vlan-pooling [wtp-group|round-robin|...]
set vlanid {integer}
set voice-enterprise [disable|enable]
set webfilter-profile {string}
next
end

```

## config wireless-controller vap

Parameter	Description	Type	Size	Default
access-control-list	Profile name for access-control-list.	string	Maximum length: 35	
additional-akms	Additional AKMs.	option	-	
	Option	Description		
	akm6	Use AKM suite employing PSK_SHA256.		
address-group	Address group ID.	string	Maximum length: 35	
antivirus-profile	AntiVirus profile name.	string	Maximum length: 35	
application-list	Application control list name.	string	Maximum length: 35	

Parameter	Description	Type	Size	Default								
atf-weight	Airtime weight in percentage.	integer	Minimum value: 0 Maximum value: 100	20								
auth	Authentication protocol.	option	-	psk								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>psk</td><td>Use a single Pre-shard Key (PSK) to authenticate all users.</td></tr><tr><td>radius</td><td>Use a RADIUS server to authenticate clients.</td></tr><tr><td>usergroup</td><td>Use a firewall usergroup to authenticate clients.</td></tr></table>				Option	Description	psk	Use a single Pre-shard Key (PSK) to authenticate all users.	radius	Use a RADIUS server to authenticate clients.	usergroup	Use a firewall usergroup to authenticate clients.
	Option	Description										
	psk	Use a single Pre-shard Key (PSK) to authenticate all users.										
	radius	Use a RADIUS server to authenticate clients.										
usergroup	Use a firewall usergroup to authenticate clients.											
auth-cert	HTTPS server certificate.	string	Maximum length: 35									
auth-portal-addr	Address of captive portal.	string	Maximum length: 63									
beacon-advertising	Fortinet beacon advertising IE data .	option	-									
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>name</td><td>AP name.</td></tr><tr><td>model</td><td>AP model abbreviation.</td></tr><tr><td>serial-number</td><td>AP serial number.</td></tr></table>				Option	Description	name	AP name.	model	AP model abbreviation.	serial-number	AP serial number.
	Option	Description										
	name	AP name.										
	model	AP model abbreviation.										
serial-number	AP serial number.											
broadcast-ssid	Enable/disable broadcasting the SSID.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable broadcasting the SSID.</td></tr><tr><td>disable</td><td>Disable broadcasting the SSID.</td></tr></table>				Option	Description	enable	Enable broadcasting the SSID.	disable	Disable broadcasting the SSID.		
	Option	Description										
	enable	Enable broadcasting the SSID.										
disable	Disable broadcasting the SSID.											
broadcast-suppression	Optional suppression of broadcast messages. For example, you can keep DHCP messages, ARP broadcasts, and so on off of the wireless network.	option	-	dhcp-up dhcp-ucast arp-known								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>dhcp-up</td><td>Suppress broadcast uplink DHCP messages.</td></tr><tr><td>dhcp-down</td><td>Suppress broadcast downlink DHCP messages.</td></tr><tr><td>dhcp-starvation</td><td>Suppress broadcast DHCP starvation req messages.</td></tr></table>				Option	Description	dhcp-up	Suppress broadcast uplink DHCP messages.	dhcp-down	Suppress broadcast downlink DHCP messages.	dhcp-starvation	Suppress broadcast DHCP starvation req messages.
	Option	Description										
	dhcp-up	Suppress broadcast uplink DHCP messages.										
	dhcp-down	Suppress broadcast downlink DHCP messages.										
dhcp-starvation	Suppress broadcast DHCP starvation req messages.											

Parameter	Description	Type	Size	Default																								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>dhcp-ucast</i></td><td>Convert downlink broadcast DHCP messages to unicast messages.</td></tr><tr><td><i>arp-known</i></td><td>Suppress broadcast ARP for known wireless clients.</td></tr><tr><td><i>arp-unknown</i></td><td>Suppress broadcast ARP for unknown wireless clients.</td></tr><tr><td><i>arp-reply</i></td><td>Suppress broadcast ARP reply from wireless clients.</td></tr><tr><td><i>arp-poison</i></td><td>Suppress ARP poison messages from wireless clients.</td></tr><tr><td><i>arp-proxy</i></td><td>Reply ARP requests for wireless clients as a proxy.</td></tr><tr><td><i>netbios-ns</i></td><td>Suppress NetBIOS name services packets with UDP port 137.</td></tr><tr><td><i>netbios-ds</i></td><td>Suppress NetBIOS datagram services packets with UDP port 138.</td></tr><tr><td><i>ipv6</i></td><td>Suppress IPv6 packets.</td></tr><tr><td><i>all-other-mc</i></td><td>Suppress all other multicast messages.</td></tr><tr><td><i>all-other-bc</i></td><td>Suppress all other broadcast messages.</td></tr></table>	Option	Description	<i>dhcp-ucast</i>	Convert downlink broadcast DHCP messages to unicast messages.	<i>arp-known</i>	Suppress broadcast ARP for known wireless clients.	<i>arp-unknown</i>	Suppress broadcast ARP for unknown wireless clients.	<i>arp-reply</i>	Suppress broadcast ARP reply from wireless clients.	<i>arp-poison</i>	Suppress ARP poison messages from wireless clients.	<i>arp-proxy</i>	Reply ARP requests for wireless clients as a proxy.	<i>netbios-ns</i>	Suppress NetBIOS name services packets with UDP port 137.	<i>netbios-ds</i>	Suppress NetBIOS datagram services packets with UDP port 138.	<i>ipv6</i>	Suppress IPv6 packets.	<i>all-other-mc</i>	Suppress all other multicast messages.	<i>all-other-bc</i>	Suppress all other broadcast messages.			
	Option	Description																										
	<i>dhcp-ucast</i>	Convert downlink broadcast DHCP messages to unicast messages.																										
	<i>arp-known</i>	Suppress broadcast ARP for known wireless clients.																										
	<i>arp-unknown</i>	Suppress broadcast ARP for unknown wireless clients.																										
	<i>arp-reply</i>	Suppress broadcast ARP reply from wireless clients.																										
	<i>arp-poison</i>	Suppress ARP poison messages from wireless clients.																										
	<i>arp-proxy</i>	Reply ARP requests for wireless clients as a proxy.																										
	<i>netbios-ns</i>	Suppress NetBIOS name services packets with UDP port 137.																										
	<i>netbios-ds</i>	Suppress NetBIOS datagram services packets with UDP port 138.																										
	<i>ipv6</i>	Suppress IPv6 packets.																										
	<i>all-other-mc</i>	Suppress all other multicast messages.																										
<i>all-other-bc</i>	Suppress all other broadcast messages.																											
bss-color-partial	Enable/disable 802.11ax partial BSS color.	option	-	enable																								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable 802.11ax partial BSS color.</td></tr><tr><td><i>disable</i></td><td>Disable 802.11ax partial BSS color.</td></tr></table>	Option	Description	<i>enable</i>	Enable 802.11ax partial BSS color.	<i>disable</i>	Disable 802.11ax partial BSS color.																					
	Option	Description																										
	<i>enable</i>	Enable 802.11ax partial BSS color.																										
<i>disable</i>	Disable 802.11ax partial BSS color.																											
bstm-disassociation-imminent	Enable/disable forcing of disassociation after the BSTM request timer has been reached.	option	-	enable																								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable BSTM disassociation imminent.</td></tr><tr><td><i>disable</i></td><td>Disable BSTM disassociation imminent.</td></tr></table>	Option	Description	<i>enable</i>	Enable BSTM disassociation imminent.	<i>disable</i>	Disable BSTM disassociation imminent.																					
	Option	Description																										
	<i>enable</i>	Enable BSTM disassociation imminent.																										
<i>disable</i>	Disable BSTM disassociation imminent.																											
bstm-load-balancing-disassoc-timer	Time interval for client to voluntarily leave AP before forcing a disassociation due to AP load-balancing.	integer	Minimum value: 1 Maximum value: 30	10																								
bstm-rssi-disassoc-timer	Time interval for client to voluntarily leave AP before forcing a disassociation due to low RSSI.	integer	Minimum value: 1 Maximum value: 2000	200																								
captive-portal-ac-name	Local-bridging captive portal ac-name.	string	Maximum length: 35																									



Parameter	Description	Type	Size	Default										
captive-portal-auth-timeout	Hard timeout - AP will always clear the session after timeout regardless of traffic.	integer	Minimum value: 0 Maximum value: 864000	0										
dhcp-address-enforcement	Enable/disable DHCP address enforcement.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable DHCP enforcement, data from clients that have not completed the DHCP process will be blocked.</td></tr><tr><td><i>disable</i></td><td>Disable DHCP enforcement, clients can access the network without DHCP process.</td></tr></table>				Option	Description	<i>enable</i>	Enable DHCP enforcement, data from clients that have not completed the DHCP process will be blocked.	<i>disable</i>	Disable DHCP enforcement, clients can access the network without DHCP process.				
	Option	Description												
	<i>enable</i>	Enable DHCP enforcement, data from clients that have not completed the DHCP process will be blocked.												
<i>disable</i>	Disable DHCP enforcement, clients can access the network without DHCP process.													
dhcp-lease-time	DHCP lease time in seconds for NAT IP address.	integer	Minimum value: 300 Maximum value: 8640000	2400										
dhcp-option43-insertion	Enable/disable insertion of DHCP option 43.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable insertion of DHCP option 43.</td></tr><tr><td><i>disable</i></td><td>Disable insertion of DHCP option 43.</td></tr></table>				Option	Description	<i>enable</i>	Enable insertion of DHCP option 43.	<i>disable</i>	Disable insertion of DHCP option 43.				
	Option	Description												
	<i>enable</i>	Enable insertion of DHCP option 43.												
<i>disable</i>	Disable insertion of DHCP option 43.													
dhcp-option82-circuit-id-insertion	Enable/disable DHCP option 82 circuit-id insert.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>style-1</i></td><td>ASCII string composed of AP-MAC;SSID;SSID-TYPE. For example, "xx:xx:xx:xx:xx:xx;wifi;s".</td></tr><tr><td><i>style-2</i></td><td>ASCII string composed of AP-MAC. For example, "xx:xx:xx:xx:xx:xx".</td></tr><tr><td><i>style-3</i></td><td>ASCII string composed of NETWORK-TYPE:WTPPROF-NAME:VLAN:SSID:AP-MODEL:AP-HOSTNAME:AP-MAC. For example,"WLAN:FAPS221E-default:100:wifi:PS221E:FortiAP-S221E:xx:xx:xx:xx:xx:xx".</td></tr><tr><td><i>disable</i></td><td>Disable DHCP option 82 circuit-id insert.</td></tr></table>				Option	Description	<i>style-1</i>	ASCII string composed of AP-MAC;SSID;SSID-TYPE. For example, "xx:xx:xx:xx:xx:xx;wifi;s".	<i>style-2</i>	ASCII string composed of AP-MAC. For example, "xx:xx:xx:xx:xx:xx".	<i>style-3</i>	ASCII string composed of NETWORK-TYPE:WTPPROF-NAME:VLAN:SSID:AP-MODEL:AP-HOSTNAME:AP-MAC. For example,"WLAN:FAPS221E-default:100:wifi:PS221E:FortiAP-S221E:xx:xx:xx:xx:xx:xx".	<i>disable</i>	Disable DHCP option 82 circuit-id insert.
	Option	Description												
	<i>style-1</i>	ASCII string composed of AP-MAC;SSID;SSID-TYPE. For example, "xx:xx:xx:xx:xx:xx;wifi;s".												
	<i>style-2</i>	ASCII string composed of AP-MAC. For example, "xx:xx:xx:xx:xx:xx".												
	<i>style-3</i>	ASCII string composed of NETWORK-TYPE:WTPPROF-NAME:VLAN:SSID:AP-MODEL:AP-HOSTNAME:AP-MAC. For example,"WLAN:FAPS221E-default:100:wifi:PS221E:FortiAP-S221E:xx:xx:xx:xx:xx:xx".												
<i>disable</i>	Disable DHCP option 82 circuit-id insert.													
dhcp-option82-insertion	Enable/disable DHCP option 82 insert.	option	-	disable										

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable DHCP option 82 insert.</td></tr><tr><td><i>disable</i></td><td>Disable DHCP option 82 insert.</td></tr></table>	Option	Description	<i>enable</i>	Enable DHCP option 82 insert.	<i>disable</i>	Disable DHCP option 82 insert.			
	Option	Description								
	<i>enable</i>	Enable DHCP option 82 insert.								
<i>disable</i>	Disable DHCP option 82 insert.									
dhcp-option82-remote-id-insertion	Enable/disable DHCP option 82 remote-id insert.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>style-1</i></td><td>ASCII string in the format "xx:xx:xx:xx:xx:xx" containing MAC address of client device.</td></tr><tr><td><i>disable</i></td><td>Disable DHCP option 82 remote-id insert.</td></tr></table>	Option	Description	<i>style-1</i>	ASCII string in the format "xx:xx:xx:xx:xx:xx" containing MAC address of client device.	<i>disable</i>	Disable DHCP option 82 remote-id insert.			
	Option	Description								
	<i>style-1</i>	ASCII string in the format "xx:xx:xx:xx:xx:xx" containing MAC address of client device.								
<i>disable</i>	Disable DHCP option 82 remote-id insert.									
dynamic-vlan	Enable/disable dynamic VLAN assignment.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable dynamic VLAN assignment.</td></tr><tr><td><i>disable</i></td><td>Disable dynamic VLAN assignment.</td></tr></table>	Option	Description	<i>enable</i>	Enable dynamic VLAN assignment.	<i>disable</i>	Disable dynamic VLAN assignment.			
	Option	Description								
	<i>enable</i>	Enable dynamic VLAN assignment.								
<i>disable</i>	Disable dynamic VLAN assignment.									
eap-reauth	Enable/disable EAP re-authentication for WPA-Enterprise security.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable EAP re-authentication for WPA-Enterprise security.</td></tr><tr><td><i>disable</i></td><td>Disable EAP re-authentication for WPA-Enterprise security.</td></tr></table>	Option	Description	<i>enable</i>	Enable EAP re-authentication for WPA-Enterprise security.	<i>disable</i>	Disable EAP re-authentication for WPA-Enterprise security.			
	Option	Description								
	<i>enable</i>	Enable EAP re-authentication for WPA-Enterprise security.								
<i>disable</i>	Disable EAP re-authentication for WPA-Enterprise security.									
eap-reauth-intv	EAP re-authentication interval.	integer	Minimum value: 1800 Maximum value: 864000	86400						
eapol-key-retries	Enable/disable retransmission of EAPOL-Key frames.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable retransmission of EAPOL-Key frames (message 3/4 and group message 1/2).</td></tr><tr><td><i>enable</i></td><td>Enable retransmission of EAPOL-Key frames (message 3/4 and group message 1/2).</td></tr></table>	Option	Description	<i>disable</i>	Disable retransmission of EAPOL-Key frames (message 3/4 and group message 1/2).	<i>enable</i>	Enable retransmission of EAPOL-Key frames (message 3/4 and group message 1/2).			
	Option	Description								
	<i>disable</i>	Disable retransmission of EAPOL-Key frames (message 3/4 and group message 1/2).								
<i>enable</i>	Enable retransmission of EAPOL-Key frames (message 3/4 and group message 1/2).									
encrypt	Encryption protocol to use (only available when security is set to a WPA type).	option	-	AES						

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>TKIP</td><td>Use TKIP encryption.</td></tr><tr><td>AES</td><td>Use AES encryption.</td></tr><tr><td>TKIP-AES</td><td>Use TKIP and AES encryption.</td></tr></table>	Option	Description	TKIP	Use TKIP encryption.	AES	Use AES encryption.	TKIP-AES	Use TKIP and AES encryption.			
	Option	Description										
	TKIP	Use TKIP encryption.										
	AES	Use AES encryption.										
TKIP-AES	Use TKIP and AES encryption.											
external-fast-roaming	Enable/disable fast roaming or pre-authentication with external APs not managed by the FortiGate.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable fast roaming or pre-authentication with external APs.</td></tr><tr><td>disable</td><td>Disable fast roaming or pre-authentication with external APs.</td></tr></table>	Option	Description	enable	Enable fast roaming or pre-authentication with external APs.	disable	Disable fast roaming or pre-authentication with external APs.					
	Option	Description										
	enable	Enable fast roaming or pre-authentication with external APs.										
disable	Disable fast roaming or pre-authentication with external APs.											
external-logout	URL of external authentication logout server.	string	Maximum length: 127									
external-web	URL of external authentication web server.	var-string	Maximum length: 1023									
external-web-format	URL query parameter detection.	option	-	auto-detect								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>auto-detect</td><td>Automatically detect if "external-web" URL has any query parameter.</td></tr><tr><td>no-query-string</td><td>"external-web" URL does not have any query parameter.</td></tr><tr><td>partial-query-string</td><td>"external-web" URL has some query parameters.</td></tr></table>	Option	Description	auto-detect	Automatically detect if "external-web" URL has any query parameter.	no-query-string	"external-web" URL does not have any query parameter.	partial-query-string	"external-web" URL has some query parameters.			
	Option	Description										
	auto-detect	Automatically detect if "external-web" URL has any query parameter.										
	no-query-string	"external-web" URL does not have any query parameter.										
partial-query-string	"external-web" URL has some query parameters.											
fast-bss-transition	Enable/disable 802.11r Fast BSS Transition.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable 802.11r Fast BSS Transition (FT).</td></tr><tr><td>enable</td><td>Enable 802.11r Fast BSS Transition (FT).</td></tr></table>	Option	Description	disable	Disable 802.11r Fast BSS Transition (FT).	enable	Enable 802.11r Fast BSS Transition (FT).					
	Option	Description										
	disable	Disable 802.11r Fast BSS Transition (FT).										
enable	Enable 802.11r Fast BSS Transition (FT).											
fast-roaming	Enable/disable fast-roaming, or pre-authentication, where supported by clients.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable fast-roaming, or pre-authentication.</td></tr><tr><td>disable</td><td>Disable fast-roaming, or pre-authentication.</td></tr></table>	Option	Description	enable	Enable fast-roaming, or pre-authentication.	disable	Disable fast-roaming, or pre-authentication.					
	Option	Description										
	enable	Enable fast-roaming, or pre-authentication.										
disable	Disable fast-roaming, or pre-authentication.											

Parameter	Description	Type	Size	Default
ft-mobility-domain	Mobility domain identifier in FT.	integer	Minimum value: 1 Maximum value: 65535	1000
ft-over-ds	Enable/disable FT over the Distribution System (DS).	option	-	disable
	Option	Description		
	disable	Disable FT over the Distribution System (DS).		
	enable	Enable FT over the Distribution System (DS).		
ft-r0-key-lifetime	Lifetime of the PMK-R0 key in FT, 1-65535 minutes.	integer	Minimum value: 1 Maximum value: 65535	480
gas-comeback-delay	GAS comeback delay.	integer	Minimum value: 100 Maximum value: 10000	500
gas-fragmentation-limit	GAS fragmentation limit.	integer	Minimum value: 512 Maximum value: 4096	1024
gtk-rekey	Enable/disable GTK rekey for WPA security.	option	-	disable
	Option	Description		
	enable	Enable GTK rekey for WPA security.		
	disable	Disable GTK rekey for WPA security.		
gtk-rekey-intv	GTK rekey interval.	integer	Minimum value: 1800 Maximum value: 864000	86400
high-efficiency	Enable/disable 802.11ax high efficiency.	option	-	enable
	Option	Description		
	enable	Enable 802.11ax high efficiency.		
	disable	Disable 802.11ax high efficiency.		
hotspot20-profile	Hotspot 2.0 profile name.	string	Maximum length: 35	

Parameter	Description	Type	Size	Default																		
igmp-snooping	Enable/disable IGMP snooping.	option	-	disable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable IGMP snooping.</td></tr><tr><td><i>disable</i></td><td>Disable IGMP snooping.</td></tr></table>				Option	Description	<i>enable</i>	Enable IGMP snooping.	<i>disable</i>	Disable IGMP snooping.												
	Option	Description																				
	<i>enable</i>	Enable IGMP snooping.																				
<i>disable</i>	Disable IGMP snooping.																					
intra-vap-privacy	Enable/disable blocking communication between clients on the same SSID.	option	-	disable																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable intra-SSID privacy.</td></tr><tr><td><i>disable</i></td><td>Disable intra-SSID privacy.</td></tr></table>				Option	Description	<i>enable</i>	Enable intra-SSID privacy.	<i>disable</i>	Disable intra-SSID privacy.												
	Option	Description																				
	<i>enable</i>	Enable intra-SSID privacy.																				
<i>disable</i>	Disable intra-SSID privacy.																					
ip	IP address and subnet mask for the local standalone NAT subnet.	ipv4-classnet-host	Not Specified	0.0.0.0 0.0.0.0																		
ips-sensor	IPS sensor name.	string	Maximum length: 35																			
ipv6-rules	Optional rules of IPv6 packets. For example, you can keep RA, RS and so on off of the wireless network.	option	-	drop-icmp6ra drop-icmp6rs drop-llmnr6 drop-icmp6mld2 drop-dhcp6s drop-dhcp6c ndp-proxy drop-ns-dad																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>drop-icmp6ra</i></td><td>Drop ICMP6 Router Advertisement (RA) packets that originate from wireless clients.</td></tr><tr><td><i>drop-icmp6rs</i></td><td>Drop ICMP6 Router Solicitation (RS) packets to be sent to wireless clients.</td></tr><tr><td><i>drop-llmnr6</i></td><td>Drop Link-Local Multicast Name Resolution (LLMNR) packets</td></tr><tr><td><i>drop-icmp6mld2</i></td><td>Drop ICMP6 Multicast Listener Report V2 (MLD2) packets</td></tr><tr><td><i>drop-dhcp6s</i></td><td>Drop DHCP6 server generated packets that originate from wireless clients.</td></tr><tr><td><i>drop-dhcp6c</i></td><td>Drop DHCP6 client generated packets to be sent to wireless clients.</td></tr><tr><td><i>ndp-proxy</i></td><td>Enable IPv6 ndp proxy - send back na on behalf of the client and drop the ns.</td></tr><tr><td><i>drop-ns-dad</i></td><td>Drop ICMP6 NS-DAD when target address is not found in ndp proxy cache.</td></tr></table>				Option	Description	<i>drop-icmp6ra</i>	Drop ICMP6 Router Advertisement (RA) packets that originate from wireless clients.	<i>drop-icmp6rs</i>	Drop ICMP6 Router Solicitation (RS) packets to be sent to wireless clients.	<i>drop-llmnr6</i>	Drop Link-Local Multicast Name Resolution (LLMNR) packets	<i>drop-icmp6mld2</i>	Drop ICMP6 Multicast Listener Report V2 (MLD2) packets	<i>drop-dhcp6s</i>	Drop DHCP6 server generated packets that originate from wireless clients.	<i>drop-dhcp6c</i>	Drop DHCP6 client generated packets to be sent to wireless clients.	<i>ndp-proxy</i>	Enable IPv6 ndp proxy - send back na on behalf of the client and drop the ns.	<i>drop-ns-dad</i>	Drop ICMP6 NS-DAD when target address is not found in ndp proxy cache.
	Option	Description																				
	<i>drop-icmp6ra</i>	Drop ICMP6 Router Advertisement (RA) packets that originate from wireless clients.																				
	<i>drop-icmp6rs</i>	Drop ICMP6 Router Solicitation (RS) packets to be sent to wireless clients.																				
	<i>drop-llmnr6</i>	Drop Link-Local Multicast Name Resolution (LLMNR) packets																				
	<i>drop-icmp6mld2</i>	Drop ICMP6 Multicast Listener Report V2 (MLD2) packets																				
	<i>drop-dhcp6s</i>	Drop DHCP6 server generated packets that originate from wireless clients.																				
	<i>drop-dhcp6c</i>	Drop DHCP6 client generated packets to be sent to wireless clients.																				
<i>ndp-proxy</i>	Enable IPv6 ndp proxy - send back na on behalf of the client and drop the ns.																					
<i>drop-ns-dad</i>	Drop ICMP6 NS-DAD when target address is not found in ndp proxy cache.																					

Parameter	Description	Type	Size	Default										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>drop-ns-nondad</i></td><td>Drop ICMP6 NS-NonDAD when target address is not found in ndp proxy cache.</td></tr></table>	Option	Description	<i>drop-ns-nondad</i>	Drop ICMP6 NS-NonDAD when target address is not found in ndp proxy cache.									
	Option	Description												
<i>drop-ns-nondad</i>	Drop ICMP6 NS-NonDAD when target address is not found in ndp proxy cache.													
key	WEP Key.	password	Not Specified											
keyindex	WEP key index.	integer	Minimum value: 1 Maximum value: 4	1										
ldpc	VAP low-density parity-check (LDPC) coding configuration.	option	-	rxtx										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable LDPC.</td></tr><tr><td><i>rx</i></td><td>Enable LDPC when receiving traffic.</td></tr><tr><td><i>tx</i></td><td>Enable LDPC when transmitting traffic.</td></tr><tr><td><i>rxtx</i></td><td>Enable LDPC when both receiving and transmitting traffic.</td></tr></table>	Option	Description	<i>disable</i>	Disable LDPC.	<i>rx</i>	Enable LDPC when receiving traffic.	<i>tx</i>	Enable LDPC when transmitting traffic.	<i>rxtx</i>	Enable LDPC when both receiving and transmitting traffic.			
	Option	Description												
	<i>disable</i>	Disable LDPC.												
	<i>rx</i>	Enable LDPC when receiving traffic.												
	<i>tx</i>	Enable LDPC when transmitting traffic.												
<i>rxtx</i>	Enable LDPC when both receiving and transmitting traffic.													
local-authentication	Enable/disable AP local authentication.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable AP local authentication.</td></tr><tr><td><i>disable</i></td><td>Disable AP local authentication.</td></tr></table>	Option	Description	<i>enable</i>	Enable AP local authentication.	<i>disable</i>	Disable AP local authentication.							
	Option	Description												
	<i>enable</i>	Enable AP local authentication.												
<i>disable</i>	Disable AP local authentication.													
local-bridging	Enable/disable bridging of wireless and Ethernet interfaces on the FortiAP.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable AP local VAP to Ethernet bridging.</td></tr><tr><td><i>disable</i></td><td>Disable AP local VAP to Ethernet bridging.</td></tr></table>	Option	Description	<i>enable</i>	Enable AP local VAP to Ethernet bridging.	<i>disable</i>	Disable AP local VAP to Ethernet bridging.							
	Option	Description												
	<i>enable</i>	Enable AP local VAP to Ethernet bridging.												
<i>disable</i>	Disable AP local VAP to Ethernet bridging.													
local-lan	Allow/deny traffic destined for a Class A, B, or C private IP address.	option	-	allow										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow traffic destined for a Class A, B, or C private IP address.</td></tr><tr><td><i>deny</i></td><td>Deny traffic destined for a Class A, B, or C private IP address.</td></tr></table>	Option	Description	<i>allow</i>	Allow traffic destined for a Class A, B, or C private IP address.	<i>deny</i>	Deny traffic destined for a Class A, B, or C private IP address.							
	Option	Description												
	<i>allow</i>	Allow traffic destined for a Class A, B, or C private IP address.												
<i>deny</i>	Deny traffic destined for a Class A, B, or C private IP address.													
local-standalone	Enable/disable AP local standalone.	option	-	disable										

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable AP local standalone.		
	<i>disable</i>	Disable AP local standalone.		
local-standalone-dns	Enable/disable AP local standalone DNS.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable AP local standalone DNS.		
	<i>disable</i>	Disable AP local standalone DNS.		
local-standalone-dns-ip	IPv4 addresses for the local standalone DNS.	ipv4-address	Not Specified	
local-standalone-nat	Enable/disable AP local standalone NAT mode.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable AP local standalone NAT mode.		
	<i>disable</i>	Disable AP local standalone NAT mode.		
mac-auth-bypass	Enable/disable MAC authentication bypass.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable MAC authentication bypass.		
	<i>disable</i>	Disable MAC authentication bypass.		
mac-called-station-delimiter	MAC called station delimiter.	option	-	hyphen
	<b>Option</b>	<b>Description</b>		
	<i>hyphen</i>	Use hyphen as delimiter for called station.		
	<i>single-hyphen</i>	Use single hyphen as delimiter for called station.		
	<i>colon</i>	Use colon as delimiter for called station.		
	<i>none</i>	No delimiter for called station.		
mac-calling-station-delimiter	MAC calling station delimiter.	option	-	hyphen

Parameter	Description	Type	Size	Default										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>hyphen</i></td><td>Use hyphen as delimiter for calling station.</td></tr><tr><td><i>single-hyphen</i></td><td>Use single hyphen as delimiter for calling station.</td></tr><tr><td><i>colon</i></td><td>Use colon as delimiter for calling station.</td></tr><tr><td><i>none</i></td><td>No delimiter for calling station.</td></tr></table>	Option	Description	<i>hyphen</i>	Use hyphen as delimiter for calling station.	<i>single-hyphen</i>	Use single hyphen as delimiter for calling station.	<i>colon</i>	Use colon as delimiter for calling station.	<i>none</i>	No delimiter for calling station.			
	Option	Description												
	<i>hyphen</i>	Use hyphen as delimiter for calling station.												
	<i>single-hyphen</i>	Use single hyphen as delimiter for calling station.												
	<i>colon</i>	Use colon as delimiter for calling station.												
<i>none</i>	No delimiter for calling station.													
mac-case	MAC case.	option	-	uppercase										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>uppercase</i></td><td>Use uppercase MAC.</td></tr><tr><td><i>lowercase</i></td><td>Use lowercase MAC.</td></tr></table>	Option	Description	<i>uppercase</i>	Use uppercase MAC.	<i>lowercase</i>	Use lowercase MAC.							
	Option	Description												
	<i>uppercase</i>	Use uppercase MAC.												
<i>lowercase</i>	Use lowercase MAC.													
mac-filter	Enable/disable MAC filtering to block wireless clients by mac address.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable MAC filtering.</td></tr><tr><td><i>disable</i></td><td>Disable MAC filtering.</td></tr></table>	Option	Description	<i>enable</i>	Enable MAC filtering.	<i>disable</i>	Disable MAC filtering.							
	Option	Description												
	<i>enable</i>	Enable MAC filtering.												
<i>disable</i>	Disable MAC filtering.													
mac-filter-policy-other	Allow or block clients with MAC addresses that are not in the filter list.	option	-	allow										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow clients with MAC addresses that are not in the filter list.</td></tr><tr><td><i>deny</i></td><td>Block clients with MAC addresses that are not in the filter list.</td></tr></table>	Option	Description	<i>allow</i>	Allow clients with MAC addresses that are not in the filter list.	<i>deny</i>	Block clients with MAC addresses that are not in the filter list.							
	Option	Description												
	<i>allow</i>	Allow clients with MAC addresses that are not in the filter list.												
<i>deny</i>	Block clients with MAC addresses that are not in the filter list.													
mac-password-delimiter	MAC authentication password delimiter.	option	-	hyphen										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>hyphen</i></td><td>Use hyphen as delimiter for MAC auth password.</td></tr><tr><td><i>single-hyphen</i></td><td>Use single hyphen as delimiter for MAC auth password.</td></tr><tr><td><i>colon</i></td><td>Use colon as delimiter for MAC auth password.</td></tr><tr><td><i>none</i></td><td>No delimiter for MAC auth password.</td></tr></table>	Option	Description	<i>hyphen</i>	Use hyphen as delimiter for MAC auth password.	<i>single-hyphen</i>	Use single hyphen as delimiter for MAC auth password.	<i>colon</i>	Use colon as delimiter for MAC auth password.	<i>none</i>	No delimiter for MAC auth password.			
	Option	Description												
	<i>hyphen</i>	Use hyphen as delimiter for MAC auth password.												
	<i>single-hyphen</i>	Use single hyphen as delimiter for MAC auth password.												
	<i>colon</i>	Use colon as delimiter for MAC auth password.												
<i>none</i>	No delimiter for MAC auth password.													
mac-username-delimiter	MAC authentication username delimiter.	option	-	hyphen										



Parameter	Description	Type	Size	Default										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>hyphen</i></td><td>Use hyphen as delimiter for MAC auth username.</td></tr><tr><td><i>single-hyphen</i></td><td>Use single hyphen as delimiter for MAC auth username.</td></tr><tr><td><i>colon</i></td><td>Use colon as delimiter for MAC auth username.</td></tr><tr><td><i>none</i></td><td>No delimiter for MAC auth username.</td></tr></table>	Option	Description	<i>hyphen</i>	Use hyphen as delimiter for MAC auth username.	<i>single-hyphen</i>	Use single hyphen as delimiter for MAC auth username.	<i>colon</i>	Use colon as delimiter for MAC auth username.	<i>none</i>	No delimiter for MAC auth username.			
	Option	Description												
	<i>hyphen</i>	Use hyphen as delimiter for MAC auth username.												
	<i>single-hyphen</i>	Use single hyphen as delimiter for MAC auth username.												
	<i>colon</i>	Use colon as delimiter for MAC auth username.												
<i>none</i>	No delimiter for MAC auth username.													
max-clients	Maximum number of clients that can connect simultaneously to the VAP.	integer	Minimum value: 0 Maximum value: 4294967295	0										
max-clients-ap	Maximum number of clients that can connect simultaneously to the VAP per AP radio.	integer	Minimum value: 0 Maximum value: 4294967295	0										
mbo	Enable/disable Multiband Operation.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable Multiband Operation (MBO).</td></tr><tr><td><i>enable</i></td><td>Enable Multiband Operation (MBO).</td></tr></table>	Option	Description	<i>disable</i>	Disable Multiband Operation (MBO).	<i>enable</i>	Enable Multiband Operation (MBO).							
	Option	Description												
	<i>disable</i>	Disable Multiband Operation (MBO).												
<i>enable</i>	Enable Multiband Operation (MBO).													
mbo-cell-data-conn-pref	MBO cell data connection preference.	option	-	prefer-not										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>excluded</i></td><td>Wi-Fi Agile Multiband AP does not want the Wi-Fi Agile Multiband STA to use the cellular data connection.</td></tr><tr><td><i>prefer-not</i></td><td>Wi-Fi Agile Multiband AP prefers the Wi-Fi Agile Multiband STA should not use cellular data connection.</td></tr><tr><td><i>prefer-use</i></td><td>Wi-Fi Agile Multiband AP prefers the Wi-Fi Agile Multiband STA should use cellular data connection.</td></tr></table>	Option	Description	<i>excluded</i>	Wi-Fi Agile Multiband AP does not want the Wi-Fi Agile Multiband STA to use the cellular data connection.	<i>prefer-not</i>	Wi-Fi Agile Multiband AP prefers the Wi-Fi Agile Multiband STA should not use cellular data connection.	<i>prefer-use</i>	Wi-Fi Agile Multiband AP prefers the Wi-Fi Agile Multiband STA should use cellular data connection.					
	Option	Description												
	<i>excluded</i>	Wi-Fi Agile Multiband AP does not want the Wi-Fi Agile Multiband STA to use the cellular data connection.												
	<i>prefer-not</i>	Wi-Fi Agile Multiband AP prefers the Wi-Fi Agile Multiband STA should not use cellular data connection.												
<i>prefer-use</i>	Wi-Fi Agile Multiband AP prefers the Wi-Fi Agile Multiband STA should use cellular data connection.													
me-disable-thresh	Disable multicast enhancement when this many clients are receiving multicast traffic.	integer	Minimum value: 2 Maximum value: 256	32										
mesh-backhaul	Enable/disable using this VAP as a WiFi mesh backhaul. This entry is only available when security is set to a WPA type or open.	option	-	disable										

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable mesh backhaul.		
	<i>disable</i>	Disable mesh backhaul.		
mpsk-profile	MPSK profile name.	string	Maximum length: 35	
mu-mimo	Enable/disable Multi-user MIMO.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable Multi-user MIMO.		
	<i>disable</i>	Disable Multi-user MIMO.		
multicast-enhance	Enable/disable converting multicast to unicast to improve performance.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable multicast enhancement.		
	<i>disable</i>	Disable multicast enhancement.		
multicast-rate	Multicast rate.	option	-	0
	<b>Option</b>	<b>Description</b>		
	<i>0</i>	Use the default multicast rate.		
	<i>6000</i>	6 Mbps.		
	<i>12000</i>	12 Mbps.		
	<i>24000</i>	24 Mbps.		
nac	Enable/disable network access control.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable network access control.		
	<i>disable</i>	Disable network access control.		
nac-profile	NAC profile name.	string	Maximum length: 35	
name	Virtual AP name.	string	Maximum length: 15	
neighbor-report-dual-band	Enable/disable dual-band neighbor report.	option	-	disable

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable dual-band neighbor report.		
	<i>enable</i>	Enable dual-band neighbor report.		
okc	Enable/disable Opportunistic Key Caching.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable Opportunistic Key Caching (OKC).		
	<i>enable</i>	Enable Opportunistic Key Caching (OKC).		
osen	Enable/disable OSEN as part of key management.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable OSEN auth.		
	<i>disable</i>	Disable OSEN auth.		
owe-groups	OWE-Groups.	option	-	
	<b>Option</b>	<b>Description</b>		
	19	DH Group 19.		
	20	DH Group 20.		
	21	DH Group 21.		
owe-transition	Enable/disable OWE transition mode support.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable OWE transition mode support.		
	<i>enable</i>	Enable OWE transition mode support.		
owe-transition-ssid	OWE transition mode peer SSID.	string	Maximum length: 32	
passphrase	WPA pre-shared key (PSK) to be used to authenticate WiFi users.	password	Not Specified	
pmf	Protected Management Frames.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable PMF completely.		

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable PMF but deny clients without PMF.		
	<i>optional</i>	Enable PMF and allow clients without PMF.		
pmf-assoc-comeback-timeout	Protected Management Frames.	integer	Minimum value: 1 Maximum value: 20	1
pmf-sa-query-retry-timeout	Protected Management Frames.	integer	Minimum value: 1 Maximum value: 5	2
port-macauth	Enable/disable LAN port MAC authentication.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable LAN port MAC authentication.		
	<i>radius</i>	Enable LAN port RADIUS-based MAC authentication.		
	<i>address-group</i>	Enable LAN port address-group based MAC authentication.		
port-macauth-reauth-timeout	LAN port MAC authentication re-authentication timeout value.	integer	Minimum value: 120 Maximum value: 65535	7200
port-macauth-timeout	LAN port MAC authentication idle timeout value.	integer	Minimum value: 60 Maximum value: 65535	600
portal-message-override-group	Replacement message group for this VAP (only available when security is set to a captive portal type).	string	Maximum length: 35	
portal-type	Captive portal functionality. Configure how the captive portal authenticates users and whether it includes a disclaimer.	option	-	auth
	<b>Option</b>	<b>Description</b>		
	<i>auth</i>	Portal for authentication.		
	<i>auth+disclaimer</i>	Portal for authentication and disclaimer.		
	<i>disclaimer</i>	Portal for disclaimer.		

Parameter	Description	Type	Size	Default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>email-collect</i></td><td>Portal for email collection.</td></tr><tr><td><i>cmcc</i></td><td>Portal for CMCC.</td></tr><tr><td><i>cmcc-macauth</i></td><td>Portal for CMCC and MAC authentication.</td></tr><tr><td><i>auth-mac</i></td><td>Portal for authentication and MAC authentication.</td></tr><tr><td><i>external-auth</i></td><td>Portal for external portal authentication.</td></tr><tr><td><i>external-macauth</i></td><td>Portal for external portal MAC authentication.</td></tr></table>	Option	Description	<i>email-collect</i>	Portal for email collection.	<i>cmcc</i>	Portal for CMCC.	<i>cmcc-macauth</i>	Portal for CMCC and MAC authentication.	<i>auth-mac</i>	Portal for authentication and MAC authentication.	<i>external-auth</i>	Portal for external portal authentication.	<i>external-macauth</i>	Portal for external portal MAC authentication.			
	Option	Description																
	<i>email-collect</i>	Portal for email collection.																
	<i>cmcc</i>	Portal for CMCC.																
	<i>cmcc-macauth</i>	Portal for CMCC and MAC authentication.																
	<i>auth-mac</i>	Portal for authentication and MAC authentication.																
	<i>external-auth</i>	Portal for external portal authentication.																
<i>external-macauth</i>	Portal for external portal MAC authentication.																	
primary-wag-profile	Primary wireless access gateway profile name.	string	Maximum length: 35															
probe-resp-suppression	Enable/disable probe response suppression.	option	-	disable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable probe response suppression.</td></tr><tr><td><i>disable</i></td><td>Disable probe response suppression.</td></tr></table>	Option	Description	<i>enable</i>	Enable probe response suppression.	<i>disable</i>	Disable probe response suppression.											
	Option	Description																
	<i>enable</i>	Enable probe response suppression.																
<i>disable</i>	Disable probe response suppression.																	
probe-resp-threshold	Minimum signal level/threshold in dBm required for the AP response to probe requests.	string	Maximum length: 7	-80														
ptk-rekey	Enable/disable PTK rekey for WPA-Enterprise security.	option	-	disable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable PTK rekey for WPA-Enterprise security.</td></tr><tr><td><i>disable</i></td><td>Disable PTK rekey for WPA-Enterprise security.</td></tr></table>	Option	Description	<i>enable</i>	Enable PTK rekey for WPA-Enterprise security.	<i>disable</i>	Disable PTK rekey for WPA-Enterprise security.											
	Option	Description																
	<i>enable</i>	Enable PTK rekey for WPA-Enterprise security.																
<i>disable</i>	Disable PTK rekey for WPA-Enterprise security.																	
ptk-rekey-intv	PTK rekey interval.	integer	Minimum value: 1800 Maximum value: 864000	86400														
qos-profile	Quality of service profile name.	string	Maximum length: 35															
quarantine	Enable/disable station quarantine.	option	-	enable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable station quarantine.</td></tr><tr><td><i>disable</i></td><td>Disable station quarantine.</td></tr></table>	Option	Description	<i>enable</i>	Enable station quarantine.	<i>disable</i>	Disable station quarantine.											
	Option	Description																
	<i>enable</i>	Enable station quarantine.																
<i>disable</i>	Disable station quarantine.																	

Parameter	Description	Type	Size	Default						
radio-2g-threshold	Minimum signal level/threshold in dBm required for the AP response to receive a packet in 2.4G band.	string	Maximum length: 7	-79						
radio-5g-threshold	Minimum signal level/threshold in dBm required for the AP response to receive a packet in 5G band.	string	Maximum length: 7	-76						
radio-sensitivity	Enable/disable software radio sensitivity.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable software radio sensitivity.</td></tr><tr><td><i>disable</i></td><td>Disable software radio sensitivity.</td></tr></table>	Option	Description	<i>enable</i>	Enable software radio sensitivity.	<i>disable</i>	Disable software radio sensitivity.			
Option	Description									
<i>enable</i>	Enable software radio sensitivity.									
<i>disable</i>	Disable software radio sensitivity.									
radius-mac-auth	Enable/disable RADIUS-based MAC authentication of clients.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable RADIUS-based MAC authentication.</td></tr><tr><td><i>disable</i></td><td>Disable RADIUS-based MAC authentication.</td></tr></table>	Option	Description	<i>enable</i>	Enable RADIUS-based MAC authentication.	<i>disable</i>	Disable RADIUS-based MAC authentication.			
Option	Description									
<i>enable</i>	Enable RADIUS-based MAC authentication.									
<i>disable</i>	Disable RADIUS-based MAC authentication.									
radius-mac-auth-server	RADIUS-based MAC authentication server.	string	Maximum length: 35							
radius-mac-auth-usergroups <name>	Selective user groups that are permitted for RADIUS mac authentication. User group name.	string	Maximum length: 79							
radius-mac-mpsk-auth	Enable/disable RADIUS-based MAC authentication of clients for MPSK authentication.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable RADIUS-based MAC authentication for MPSK authentication.</td></tr><tr><td><i>disable</i></td><td>Disable RADIUS-based MAC authentication for MPSK authentication.</td></tr></table>	Option	Description	<i>enable</i>	Enable RADIUS-based MAC authentication for MPSK authentication.	<i>disable</i>	Disable RADIUS-based MAC authentication for MPSK authentication.			
Option	Description									
<i>enable</i>	Enable RADIUS-based MAC authentication for MPSK authentication.									
<i>disable</i>	Disable RADIUS-based MAC authentication for MPSK authentication.									
radius-mac-mpsk-timeout	RADIUS MAC MPSK cache timeout interval.	integer	Minimum value: 300 Maximum value: 864000	86400						
radius-server	RADIUS server to be used to authenticate WiFi users.	string	Maximum length: 35							
rates-11a	Allowed data rates for 802.11a.	option	-							

Parameter	Description	Type	Size	Default																																																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>1</td><td>1 Mbps supported rate.</td></tr><tr><td>1-basic</td><td>1 Mbps BSS basic rate.</td></tr><tr><td>2</td><td>2 Mbps supported rate.</td></tr><tr><td>2-basic</td><td>2 Mbps BSS basic rate.</td></tr><tr><td>5.5</td><td>5.5 Mbps supported rate.</td></tr><tr><td>5.5-basic</td><td>5.5 Mbps BSS basic rate.</td></tr><tr><td>11</td><td>11 Mbps supported rate.</td></tr><tr><td>11-basic</td><td>11 Mbps BSS basic rate.</td></tr><tr><td>6</td><td>6 Mbps supported rate.</td></tr><tr><td>6-basic</td><td>6 Mbps BSS basic rate.</td></tr><tr><td>9</td><td>9 Mbps supported rate.</td></tr><tr><td>9-basic</td><td>9 Mbps BSS basic rate.</td></tr><tr><td>12</td><td>12 Mbps supported rate.</td></tr><tr><td>12-basic</td><td>12 Mbps BSS basic rate.</td></tr><tr><td>18</td><td>18 Mbps supported rate.</td></tr><tr><td>18-basic</td><td>18 Mbps BSS basic rate.</td></tr><tr><td>24</td><td>24 Mbps supported rate.</td></tr><tr><td>24-basic</td><td>24 Mbps BSS basic rate.</td></tr><tr><td>36</td><td>36 Mbps supported rate.</td></tr><tr><td>36-basic</td><td>36 Mbps BSS basic rate.</td></tr><tr><td>48</td><td>48 Mbps supported rate.</td></tr><tr><td>48-basic</td><td>48 Mbps BSS basic rate.</td></tr><tr><td>54</td><td>54 Mbps supported rate.</td></tr><tr><td>54-basic</td><td>54 Mbps BSS basic rate.</td></tr></table>	Option	Description	1	1 Mbps supported rate.	1-basic	1 Mbps BSS basic rate.	2	2 Mbps supported rate.	2-basic	2 Mbps BSS basic rate.	5.5	5.5 Mbps supported rate.	5.5-basic	5.5 Mbps BSS basic rate.	11	11 Mbps supported rate.	11-basic	11 Mbps BSS basic rate.	6	6 Mbps supported rate.	6-basic	6 Mbps BSS basic rate.	9	9 Mbps supported rate.	9-basic	9 Mbps BSS basic rate.	12	12 Mbps supported rate.	12-basic	12 Mbps BSS basic rate.	18	18 Mbps supported rate.	18-basic	18 Mbps BSS basic rate.	24	24 Mbps supported rate.	24-basic	24 Mbps BSS basic rate.	36	36 Mbps supported rate.	36-basic	36 Mbps BSS basic rate.	48	48 Mbps supported rate.	48-basic	48 Mbps BSS basic rate.	54	54 Mbps supported rate.	54-basic	54 Mbps BSS basic rate.			
	Option	Description																																																				
	1	1 Mbps supported rate.																																																				
	1-basic	1 Mbps BSS basic rate.																																																				
	2	2 Mbps supported rate.																																																				
	2-basic	2 Mbps BSS basic rate.																																																				
	5.5	5.5 Mbps supported rate.																																																				
	5.5-basic	5.5 Mbps BSS basic rate.																																																				
	11	11 Mbps supported rate.																																																				
	11-basic	11 Mbps BSS basic rate.																																																				
	6	6 Mbps supported rate.																																																				
	6-basic	6 Mbps BSS basic rate.																																																				
	9	9 Mbps supported rate.																																																				
	9-basic	9 Mbps BSS basic rate.																																																				
	12	12 Mbps supported rate.																																																				
	12-basic	12 Mbps BSS basic rate.																																																				
	18	18 Mbps supported rate.																																																				
	18-basic	18 Mbps BSS basic rate.																																																				
	24	24 Mbps supported rate.																																																				
	24-basic	24 Mbps BSS basic rate.																																																				
	36	36 Mbps supported rate.																																																				
	36-basic	36 Mbps BSS basic rate.																																																				
	48	48 Mbps supported rate.																																																				
	48-basic	48 Mbps BSS basic rate.																																																				
	54	54 Mbps supported rate.																																																				
	54-basic	54 Mbps BSS basic rate.																																																				
rates-11ac-ss12	Allowed data rates for 802.11ac with 1 or 2 spatial streams.	option	-																																																			
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>mcs0/1</td><td>Data rate for MCS index 0 with 1 spatial stream.</td></tr></table>	Option	Description	mcs0/1	Data rate for MCS index 0 with 1 spatial stream.																																																	
	Option	Description																																																				
mcs0/1	Data rate for MCS index 0 with 1 spatial stream.																																																					

Parameter	Description	Type	Size	Default																																																	
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>mcs1/1</i></td><td>Data rate for MCS index 1 with 1 spatial stream.</td></tr><tr><td><i>mcs2/1</i></td><td>Data rate for MCS index 2 with 1 spatial stream.</td></tr><tr><td><i>mcs3/1</i></td><td>Data rate for MCS index 3 with 1 spatial stream.</td></tr><tr><td><i>mcs4/1</i></td><td>Data rate for MCS index 4 with 1 spatial stream.</td></tr><tr><td><i>mcs5/1</i></td><td>Data rate for MCS index 5 with 1 spatial stream.</td></tr><tr><td><i>mcs6/1</i></td><td>Data rate for MCS index 6 with 1 spatial stream.</td></tr><tr><td><i>mcs7/1</i></td><td>Data rate for MCS index 7 with 1 spatial stream.</td></tr><tr><td><i>mcs8/1</i></td><td>Data rate for MCS index 8 with 1 spatial stream.</td></tr><tr><td><i>mcs9/1</i></td><td>Data rate for MCS index 9 with 1 spatial stream.</td></tr><tr><td><i>mcs10/1</i></td><td>Data rate for MCS index 10 with 1 spatial stream.</td></tr><tr><td><i>mcs11/1</i></td><td>Data rate for MCS index 11 with 1 spatial stream.</td></tr><tr><td><i>mcs0/2</i></td><td>Data rate for MCS index 0 with 2 spatial streams.</td></tr><tr><td><i>mcs1/2</i></td><td>Data rate for MCS index 1 with 2 spatial streams.</td></tr><tr><td><i>mcs2/2</i></td><td>Data rate for MCS index 2 with 2 spatial streams.</td></tr><tr><td><i>mcs3/2</i></td><td>Data rate for MCS index 3 with 2 spatial streams.</td></tr><tr><td><i>mcs4/2</i></td><td>Data rate for MCS index 4 with 2 spatial streams.</td></tr><tr><td><i>mcs5/2</i></td><td>Data rate for MCS index 5 with 2 spatial streams.</td></tr><tr><td><i>mcs6/2</i></td><td>Data rate for MCS index 6 with 2 spatial streams.</td></tr><tr><td><i>mcs7/2</i></td><td>Data rate for MCS index 7 with 2 spatial streams.</td></tr><tr><td><i>mcs8/2</i></td><td>Data rate for MCS index 8 with 2 spatial streams.</td></tr><tr><td><i>mcs9/2</i></td><td>Data rate for MCS index 9 with 2 spatial streams.</td></tr><tr><td><i>mcs10/2</i></td><td>Data rate for MCS index 10 with 2 spatial streams.</td></tr><tr><td><i>mcs11/2</i></td><td>Data rate for MCS index 11 with 2 spatial streams.</td></tr></table>	Option	Description	<i>mcs1/1</i>	Data rate for MCS index 1 with 1 spatial stream.	<i>mcs2/1</i>	Data rate for MCS index 2 with 1 spatial stream.	<i>mcs3/1</i>	Data rate for MCS index 3 with 1 spatial stream.	<i>mcs4/1</i>	Data rate for MCS index 4 with 1 spatial stream.	<i>mcs5/1</i>	Data rate for MCS index 5 with 1 spatial stream.	<i>mcs6/1</i>	Data rate for MCS index 6 with 1 spatial stream.	<i>mcs7/1</i>	Data rate for MCS index 7 with 1 spatial stream.	<i>mcs8/1</i>	Data rate for MCS index 8 with 1 spatial stream.	<i>mcs9/1</i>	Data rate for MCS index 9 with 1 spatial stream.	<i>mcs10/1</i>	Data rate for MCS index 10 with 1 spatial stream.	<i>mcs11/1</i>	Data rate for MCS index 11 with 1 spatial stream.	<i>mcs0/2</i>	Data rate for MCS index 0 with 2 spatial streams.	<i>mcs1/2</i>	Data rate for MCS index 1 with 2 spatial streams.	<i>mcs2/2</i>	Data rate for MCS index 2 with 2 spatial streams.	<i>mcs3/2</i>	Data rate for MCS index 3 with 2 spatial streams.	<i>mcs4/2</i>	Data rate for MCS index 4 with 2 spatial streams.	<i>mcs5/2</i>	Data rate for MCS index 5 with 2 spatial streams.	<i>mcs6/2</i>	Data rate for MCS index 6 with 2 spatial streams.	<i>mcs7/2</i>	Data rate for MCS index 7 with 2 spatial streams.	<i>mcs8/2</i>	Data rate for MCS index 8 with 2 spatial streams.	<i>mcs9/2</i>	Data rate for MCS index 9 with 2 spatial streams.	<i>mcs10/2</i>	Data rate for MCS index 10 with 2 spatial streams.	<i>mcs11/2</i>	Data rate for MCS index 11 with 2 spatial streams.				
	Option	Description																																																			
	<i>mcs1/1</i>	Data rate for MCS index 1 with 1 spatial stream.																																																			
	<i>mcs2/1</i>	Data rate for MCS index 2 with 1 spatial stream.																																																			
	<i>mcs3/1</i>	Data rate for MCS index 3 with 1 spatial stream.																																																			
	<i>mcs4/1</i>	Data rate for MCS index 4 with 1 spatial stream.																																																			
	<i>mcs5/1</i>	Data rate for MCS index 5 with 1 spatial stream.																																																			
	<i>mcs6/1</i>	Data rate for MCS index 6 with 1 spatial stream.																																																			
	<i>mcs7/1</i>	Data rate for MCS index 7 with 1 spatial stream.																																																			
	<i>mcs8/1</i>	Data rate for MCS index 8 with 1 spatial stream.																																																			
	<i>mcs9/1</i>	Data rate for MCS index 9 with 1 spatial stream.																																																			
	<i>mcs10/1</i>	Data rate for MCS index 10 with 1 spatial stream.																																																			
	<i>mcs11/1</i>	Data rate for MCS index 11 with 1 spatial stream.																																																			
	<i>mcs0/2</i>	Data rate for MCS index 0 with 2 spatial streams.																																																			
	<i>mcs1/2</i>	Data rate for MCS index 1 with 2 spatial streams.																																																			
	<i>mcs2/2</i>	Data rate for MCS index 2 with 2 spatial streams.																																																			
	<i>mcs3/2</i>	Data rate for MCS index 3 with 2 spatial streams.																																																			
	<i>mcs4/2</i>	Data rate for MCS index 4 with 2 spatial streams.																																																			
	<i>mcs5/2</i>	Data rate for MCS index 5 with 2 spatial streams.																																																			
	<i>mcs6/2</i>	Data rate for MCS index 6 with 2 spatial streams.																																																			
	<i>mcs7/2</i>	Data rate for MCS index 7 with 2 spatial streams.																																																			
	<i>mcs8/2</i>	Data rate for MCS index 8 with 2 spatial streams.																																																			
	<i>mcs9/2</i>	Data rate for MCS index 9 with 2 spatial streams.																																																			
<i>mcs10/2</i>	Data rate for MCS index 10 with 2 spatial streams.																																																				
<i>mcs11/2</i>	Data rate for MCS index 11 with 2 spatial streams.																																																				
rates-11ac-ss34	Allowed data rates for 802.11ac with 3 or 4 spatial streams.	option	-																																																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>mcs0/3</i></td><td>Data rate for MCS index 0 with 3 spatial streams.</td></tr><tr><td><i>mcs1/3</i></td><td>Data rate for MCS index 1 with 3 spatial streams.</td></tr></table>	Option	Description	<i>mcs0/3</i>	Data rate for MCS index 0 with 3 spatial streams.	<i>mcs1/3</i>	Data rate for MCS index 1 with 3 spatial streams.																																														
	Option	Description																																																			
	<i>mcs0/3</i>	Data rate for MCS index 0 with 3 spatial streams.																																																			
<i>mcs1/3</i>	Data rate for MCS index 1 with 3 spatial streams.																																																				



Parameter	Description	Type	Size	Default																																															
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>mcs2/3</i></td><td>Data rate for MCS index 2 with 3 spatial streams.</td></tr><tr><td><i>mcs3/3</i></td><td>Data rate for MCS index 3 with 3 spatial streams.</td></tr><tr><td><i>mcs4/3</i></td><td>Data rate for MCS index 4 with 3 spatial streams.</td></tr><tr><td><i>mcs5/3</i></td><td>Data rate for MCS index 5 with 3 spatial streams.</td></tr><tr><td><i>mcs6/3</i></td><td>Data rate for MCS index 6 with 3 spatial streams.</td></tr><tr><td><i>mcs7/3</i></td><td>Data rate for MCS index 7 with 3 spatial streams.</td></tr><tr><td><i>mcs8/3</i></td><td>Data rate for MCS index 8 with 3 spatial streams.</td></tr><tr><td><i>mcs9/3</i></td><td>Data rate for MCS index 9 with 3 spatial streams.</td></tr><tr><td><i>mcs10/3</i></td><td>Data rate for MCS index 10 with 3 spatial streams.</td></tr><tr><td><i>mcs11/3</i></td><td>Data rate for MCS index 11 with 3 spatial streams.</td></tr><tr><td><i>mcs0/4</i></td><td>Data rate for MCS index 0 with 4 spatial streams.</td></tr><tr><td><i>mcs1/4</i></td><td>Data rate for MCS index 1 with 4 spatial streams.</td></tr><tr><td><i>mcs2/4</i></td><td>Data rate for MCS index 2 with 4 spatial streams.</td></tr><tr><td><i>mcs3/4</i></td><td>Data rate for MCS index 3 with 4 spatial streams.</td></tr><tr><td><i>mcs4/4</i></td><td>Data rate for MCS index 4 with 4 spatial streams.</td></tr><tr><td><i>mcs5/4</i></td><td>Data rate for MCS index 5 with 4 spatial streams.</td></tr><tr><td><i>mcs6/4</i></td><td>Data rate for MCS index 6 with 4 spatial streams.</td></tr><tr><td><i>mcs7/4</i></td><td>Data rate for MCS index 7 with 4 spatial streams.</td></tr><tr><td><i>mcs8/4</i></td><td>Data rate for MCS index 8 with 4 spatial streams.</td></tr><tr><td><i>mcs9/4</i></td><td>Data rate for MCS index 9 with 4 spatial streams.</td></tr><tr><td><i>mcs10/4</i></td><td>Data rate for MCS index 10 with 4 spatial streams.</td></tr><tr><td><i>mcs11/4</i></td><td>Data rate for MCS index 11 with 4 spatial streams.</td></tr></table>	Option	Description	<i>mcs2/3</i>	Data rate for MCS index 2 with 3 spatial streams.	<i>mcs3/3</i>	Data rate for MCS index 3 with 3 spatial streams.	<i>mcs4/3</i>	Data rate for MCS index 4 with 3 spatial streams.	<i>mcs5/3</i>	Data rate for MCS index 5 with 3 spatial streams.	<i>mcs6/3</i>	Data rate for MCS index 6 with 3 spatial streams.	<i>mcs7/3</i>	Data rate for MCS index 7 with 3 spatial streams.	<i>mcs8/3</i>	Data rate for MCS index 8 with 3 spatial streams.	<i>mcs9/3</i>	Data rate for MCS index 9 with 3 spatial streams.	<i>mcs10/3</i>	Data rate for MCS index 10 with 3 spatial streams.	<i>mcs11/3</i>	Data rate for MCS index 11 with 3 spatial streams.	<i>mcs0/4</i>	Data rate for MCS index 0 with 4 spatial streams.	<i>mcs1/4</i>	Data rate for MCS index 1 with 4 spatial streams.	<i>mcs2/4</i>	Data rate for MCS index 2 with 4 spatial streams.	<i>mcs3/4</i>	Data rate for MCS index 3 with 4 spatial streams.	<i>mcs4/4</i>	Data rate for MCS index 4 with 4 spatial streams.	<i>mcs5/4</i>	Data rate for MCS index 5 with 4 spatial streams.	<i>mcs6/4</i>	Data rate for MCS index 6 with 4 spatial streams.	<i>mcs7/4</i>	Data rate for MCS index 7 with 4 spatial streams.	<i>mcs8/4</i>	Data rate for MCS index 8 with 4 spatial streams.	<i>mcs9/4</i>	Data rate for MCS index 9 with 4 spatial streams.	<i>mcs10/4</i>	Data rate for MCS index 10 with 4 spatial streams.	<i>mcs11/4</i>	Data rate for MCS index 11 with 4 spatial streams.				
	Option	Description																																																	
	<i>mcs2/3</i>	Data rate for MCS index 2 with 3 spatial streams.																																																	
	<i>mcs3/3</i>	Data rate for MCS index 3 with 3 spatial streams.																																																	
	<i>mcs4/3</i>	Data rate for MCS index 4 with 3 spatial streams.																																																	
	<i>mcs5/3</i>	Data rate for MCS index 5 with 3 spatial streams.																																																	
	<i>mcs6/3</i>	Data rate for MCS index 6 with 3 spatial streams.																																																	
	<i>mcs7/3</i>	Data rate for MCS index 7 with 3 spatial streams.																																																	
	<i>mcs8/3</i>	Data rate for MCS index 8 with 3 spatial streams.																																																	
	<i>mcs9/3</i>	Data rate for MCS index 9 with 3 spatial streams.																																																	
	<i>mcs10/3</i>	Data rate for MCS index 10 with 3 spatial streams.																																																	
	<i>mcs11/3</i>	Data rate for MCS index 11 with 3 spatial streams.																																																	
	<i>mcs0/4</i>	Data rate for MCS index 0 with 4 spatial streams.																																																	
	<i>mcs1/4</i>	Data rate for MCS index 1 with 4 spatial streams.																																																	
	<i>mcs2/4</i>	Data rate for MCS index 2 with 4 spatial streams.																																																	
	<i>mcs3/4</i>	Data rate for MCS index 3 with 4 spatial streams.																																																	
	<i>mcs4/4</i>	Data rate for MCS index 4 with 4 spatial streams.																																																	
	<i>mcs5/4</i>	Data rate for MCS index 5 with 4 spatial streams.																																																	
	<i>mcs6/4</i>	Data rate for MCS index 6 with 4 spatial streams.																																																	
	<i>mcs7/4</i>	Data rate for MCS index 7 with 4 spatial streams.																																																	
<i>mcs8/4</i>	Data rate for MCS index 8 with 4 spatial streams.																																																		
<i>mcs9/4</i>	Data rate for MCS index 9 with 4 spatial streams.																																																		
<i>mcs10/4</i>	Data rate for MCS index 10 with 4 spatial streams.																																																		
<i>mcs11/4</i>	Data rate for MCS index 11 with 4 spatial streams.																																																		
rates-11ax-ss12	Allowed data rates for 802.11ax with 1 or 2 spatial streams.	option	-																																																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>mcs0/1</i></td><td>Data rate for MCS index 0 with 1 spatial stream.</td></tr><tr><td><i>mcs1/1</i></td><td>Data rate for MCS index 1 with 1 spatial stream.</td></tr><tr><td><i>mcs2/1</i></td><td>Data rate for MCS index 2 with 1 spatial stream.</td></tr></table>	Option	Description	<i>mcs0/1</i>	Data rate for MCS index 0 with 1 spatial stream.	<i>mcs1/1</i>	Data rate for MCS index 1 with 1 spatial stream.	<i>mcs2/1</i>	Data rate for MCS index 2 with 1 spatial stream.																																										
	Option	Description																																																	
	<i>mcs0/1</i>	Data rate for MCS index 0 with 1 spatial stream.																																																	
	<i>mcs1/1</i>	Data rate for MCS index 1 with 1 spatial stream.																																																	
<i>mcs2/1</i>	Data rate for MCS index 2 with 1 spatial stream.																																																		

Parameter	Description	Type	Size	Default																																												
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>mcs3/1</i></td><td>Data rate for MCS index 3 with 1 spatial stream.</td></tr><tr><td><i>mcs4/1</i></td><td>Data rate for MCS index 4 with 1 spatial stream.</td></tr><tr><td><i>mcs5/1</i></td><td>Data rate for MCS index 5 with 1 spatial stream.</td></tr><tr><td><i>mcs6/1</i></td><td>Data rate for MCS index 6 with 1 spatial stream.</td></tr><tr><td><i>mcs7/1</i></td><td>Data rate for MCS index 7 with 1 spatial stream.</td></tr><tr><td><i>mcs8/1</i></td><td>Data rate for MCS index 8 with 1 spatial stream.</td></tr><tr><td><i>mcs9/1</i></td><td>Data rate for MCS index 9 with 1 spatial stream.</td></tr><tr><td><i>mcs10/1</i></td><td>Data rate for MCS index 10 with 1 spatial stream.</td></tr><tr><td><i>mcs11/1</i></td><td>Data rate for MCS index 11 with 1 spatial stream.</td></tr><tr><td><i>mcs0/2</i></td><td>Data rate for MCS index 0 with 2 spatial streams.</td></tr><tr><td><i>mcs1/2</i></td><td>Data rate for MCS index 1 with 2 spatial streams.</td></tr><tr><td><i>mcs2/2</i></td><td>Data rate for MCS index 2 with 2 spatial streams.</td></tr><tr><td><i>mcs3/2</i></td><td>Data rate for MCS index 3 with 2 spatial streams.</td></tr><tr><td><i>mcs4/2</i></td><td>Data rate for MCS index 4 with 2 spatial streams.</td></tr><tr><td><i>mcs5/2</i></td><td>Data rate for MCS index 5 with 2 spatial streams.</td></tr><tr><td><i>mcs6/2</i></td><td>Data rate for MCS index 6 with 2 spatial streams.</td></tr><tr><td><i>mcs7/2</i></td><td>Data rate for MCS index 7 with 2 spatial streams.</td></tr><tr><td><i>mcs8/2</i></td><td>Data rate for MCS index 8 with 2 spatial streams.</td></tr><tr><td><i>mcs9/2</i></td><td>Data rate for MCS index 9 with 2 spatial streams.</td></tr><tr><td><i>mcs10/2</i></td><td>Data rate for MCS index 10 with 2 spatial streams.</td></tr><tr><td><i>mcs11/2</i></td><td>Data rate for MCS index 11 with 2 spatial streams.</td></tr></table>	Option	Description	<i>mcs3/1</i>	Data rate for MCS index 3 with 1 spatial stream.	<i>mcs4/1</i>	Data rate for MCS index 4 with 1 spatial stream.	<i>mcs5/1</i>	Data rate for MCS index 5 with 1 spatial stream.	<i>mcs6/1</i>	Data rate for MCS index 6 with 1 spatial stream.	<i>mcs7/1</i>	Data rate for MCS index 7 with 1 spatial stream.	<i>mcs8/1</i>	Data rate for MCS index 8 with 1 spatial stream.	<i>mcs9/1</i>	Data rate for MCS index 9 with 1 spatial stream.	<i>mcs10/1</i>	Data rate for MCS index 10 with 1 spatial stream.	<i>mcs11/1</i>	Data rate for MCS index 11 with 1 spatial stream.	<i>mcs0/2</i>	Data rate for MCS index 0 with 2 spatial streams.	<i>mcs1/2</i>	Data rate for MCS index 1 with 2 spatial streams.	<i>mcs2/2</i>	Data rate for MCS index 2 with 2 spatial streams.	<i>mcs3/2</i>	Data rate for MCS index 3 with 2 spatial streams.	<i>mcs4/2</i>	Data rate for MCS index 4 with 2 spatial streams.	<i>mcs5/2</i>	Data rate for MCS index 5 with 2 spatial streams.	<i>mcs6/2</i>	Data rate for MCS index 6 with 2 spatial streams.	<i>mcs7/2</i>	Data rate for MCS index 7 with 2 spatial streams.	<i>mcs8/2</i>	Data rate for MCS index 8 with 2 spatial streams.	<i>mcs9/2</i>	Data rate for MCS index 9 with 2 spatial streams.	<i>mcs10/2</i>	Data rate for MCS index 10 with 2 spatial streams.	<i>mcs11/2</i>	Data rate for MCS index 11 with 2 spatial streams.			
	Option	Description																																														
	<i>mcs3/1</i>	Data rate for MCS index 3 with 1 spatial stream.																																														
	<i>mcs4/1</i>	Data rate for MCS index 4 with 1 spatial stream.																																														
	<i>mcs5/1</i>	Data rate for MCS index 5 with 1 spatial stream.																																														
	<i>mcs6/1</i>	Data rate for MCS index 6 with 1 spatial stream.																																														
	<i>mcs7/1</i>	Data rate for MCS index 7 with 1 spatial stream.																																														
	<i>mcs8/1</i>	Data rate for MCS index 8 with 1 spatial stream.																																														
	<i>mcs9/1</i>	Data rate for MCS index 9 with 1 spatial stream.																																														
	<i>mcs10/1</i>	Data rate for MCS index 10 with 1 spatial stream.																																														
	<i>mcs11/1</i>	Data rate for MCS index 11 with 1 spatial stream.																																														
	<i>mcs0/2</i>	Data rate for MCS index 0 with 2 spatial streams.																																														
	<i>mcs1/2</i>	Data rate for MCS index 1 with 2 spatial streams.																																														
	<i>mcs2/2</i>	Data rate for MCS index 2 with 2 spatial streams.																																														
	<i>mcs3/2</i>	Data rate for MCS index 3 with 2 spatial streams.																																														
	<i>mcs4/2</i>	Data rate for MCS index 4 with 2 spatial streams.																																														
	<i>mcs5/2</i>	Data rate for MCS index 5 with 2 spatial streams.																																														
	<i>mcs6/2</i>	Data rate for MCS index 6 with 2 spatial streams.																																														
	<i>mcs7/2</i>	Data rate for MCS index 7 with 2 spatial streams.																																														
	<i>mcs8/2</i>	Data rate for MCS index 8 with 2 spatial streams.																																														
<i>mcs9/2</i>	Data rate for MCS index 9 with 2 spatial streams.																																															
<i>mcs10/2</i>	Data rate for MCS index 10 with 2 spatial streams.																																															
<i>mcs11/2</i>	Data rate for MCS index 11 with 2 spatial streams.																																															
rates-11ax-ss34	Allowed data rates for 802.11ax with 3 or 4 spatial streams.	option	-																																													
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>mcs0/3</i></td><td>Data rate for MCS index 0 with 3 spatial streams.</td></tr><tr><td><i>mcs1/3</i></td><td>Data rate for MCS index 1 with 3 spatial streams.</td></tr><tr><td><i>mcs2/3</i></td><td>Data rate for MCS index 2 with 3 spatial streams.</td></tr><tr><td><i>mcs3/3</i></td><td>Data rate for MCS index 3 with 3 spatial streams.</td></tr></table>	Option	Description	<i>mcs0/3</i>	Data rate for MCS index 0 with 3 spatial streams.	<i>mcs1/3</i>	Data rate for MCS index 1 with 3 spatial streams.	<i>mcs2/3</i>	Data rate for MCS index 2 with 3 spatial streams.	<i>mcs3/3</i>	Data rate for MCS index 3 with 3 spatial streams.																																					
	Option	Description																																														
	<i>mcs0/3</i>	Data rate for MCS index 0 with 3 spatial streams.																																														
	<i>mcs1/3</i>	Data rate for MCS index 1 with 3 spatial streams.																																														
	<i>mcs2/3</i>	Data rate for MCS index 2 with 3 spatial streams.																																														
<i>mcs3/3</i>	Data rate for MCS index 3 with 3 spatial streams.																																															

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>mcs4/3</i>	Data rate for MCS index 4 with 3 spatial streams.		
	<i>mcs5/3</i>	Data rate for MCS index 5 with 3 spatial streams.		
	<i>mcs6/3</i>	Data rate for MCS index 6 with 3 spatial streams.		
	<i>mcs7/3</i>	Data rate for MCS index 7 with 3 spatial streams.		
	<i>mcs8/3</i>	Data rate for MCS index 8 with 3 spatial streams.		
	<i>mcs9/3</i>	Data rate for MCS index 9 with 3 spatial streams.		
	<i>mcs10/3</i>	Data rate for MCS index 10 with 3 spatial streams.		
	<i>mcs11/3</i>	Data rate for MCS index 11 with 3 spatial streams.		
	<i>mcs0/4</i>	Data rate for MCS index 0 with 4 spatial streams.		
	<i>mcs1/4</i>	Data rate for MCS index 1 with 4 spatial streams.		
	<i>mcs2/4</i>	Data rate for MCS index 2 with 4 spatial streams.		
	<i>mcs3/4</i>	Data rate for MCS index 3 with 4 spatial streams.		
	<i>mcs4/4</i>	Data rate for MCS index 4 with 4 spatial streams.		
	<i>mcs5/4</i>	Data rate for MCS index 5 with 4 spatial streams.		
	<i>mcs6/4</i>	Data rate for MCS index 6 with 4 spatial streams.		
	<i>mcs7/4</i>	Data rate for MCS index 7 with 4 spatial streams.		
	<i>mcs8/4</i>	Data rate for MCS index 8 with 4 spatial streams.		
	<i>mcs9/4</i>	Data rate for MCS index 9 with 4 spatial streams.		
	<i>mcs10/4</i>	Data rate for MCS index 10 with 4 spatial streams.		
<i>mcs11/4</i>	Data rate for MCS index 11 with 4 spatial streams.			
rates-11bg	Allowed data rates for 802.11b/g.	option	-	
	<b>Option</b>	<b>Description</b>		
	1	1 Mbps supported rate.		
	1-basic	1 Mbps BSS basic rate.		
	2	2 Mbps supported rate.		
	2-basic	2 Mbps BSS basic rate.		
	5.5	5.5 Mbps supported rate.		
	5.5-basic	5.5 Mbps BSS basic rate.		

Parameter	Description	Type	Size	Default																																							
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>11</td><td>11 Mbps supported rate.</td></tr><tr><td>11-basic</td><td>11 Mbps BSS basic rate.</td></tr><tr><td>6</td><td>6 Mbps supported rate.</td></tr><tr><td>6-basic</td><td>6 Mbps BSS basic rate.</td></tr><tr><td>9</td><td>9 Mbps supported rate.</td></tr><tr><td>9-basic</td><td>9 Mbps BSS basic rate.</td></tr><tr><td>12</td><td>12 Mbps supported rate.</td></tr><tr><td>12-basic</td><td>12 Mbps BSS basic rate.</td></tr><tr><td>18</td><td>18 Mbps supported rate.</td></tr><tr><td>18-basic</td><td>18 Mbps BSS basic rate.</td></tr><tr><td>24</td><td>24 Mbps supported rate.</td></tr><tr><td>24-basic</td><td>24 Mbps BSS basic rate.</td></tr><tr><td>36</td><td>36 Mbps supported rate.</td></tr><tr><td>36-basic</td><td>36 Mbps BSS basic rate.</td></tr><tr><td>48</td><td>48 Mbps supported rate.</td></tr><tr><td>48-basic</td><td>48 Mbps BSS basic rate.</td></tr><tr><td>54</td><td>54 Mbps supported rate.</td></tr><tr><td>54-basic</td><td>54 Mbps BSS basic rate.</td></tr></table>	Option	Description	11	11 Mbps supported rate.	11-basic	11 Mbps BSS basic rate.	6	6 Mbps supported rate.	6-basic	6 Mbps BSS basic rate.	9	9 Mbps supported rate.	9-basic	9 Mbps BSS basic rate.	12	12 Mbps supported rate.	12-basic	12 Mbps BSS basic rate.	18	18 Mbps supported rate.	18-basic	18 Mbps BSS basic rate.	24	24 Mbps supported rate.	24-basic	24 Mbps BSS basic rate.	36	36 Mbps supported rate.	36-basic	36 Mbps BSS basic rate.	48	48 Mbps supported rate.	48-basic	48 Mbps BSS basic rate.	54	54 Mbps supported rate.	54-basic	54 Mbps BSS basic rate.				
	Option	Description																																									
	11	11 Mbps supported rate.																																									
	11-basic	11 Mbps BSS basic rate.																																									
	6	6 Mbps supported rate.																																									
	6-basic	6 Mbps BSS basic rate.																																									
	9	9 Mbps supported rate.																																									
	9-basic	9 Mbps BSS basic rate.																																									
	12	12 Mbps supported rate.																																									
	12-basic	12 Mbps BSS basic rate.																																									
	18	18 Mbps supported rate.																																									
	18-basic	18 Mbps BSS basic rate.																																									
	24	24 Mbps supported rate.																																									
	24-basic	24 Mbps BSS basic rate.																																									
	36	36 Mbps supported rate.																																									
	36-basic	36 Mbps BSS basic rate.																																									
	48	48 Mbps supported rate.																																									
	48-basic	48 Mbps BSS basic rate.																																									
54	54 Mbps supported rate.																																										
54-basic	54 Mbps BSS basic rate.																																										
rates-11n-ss12	Allowed data rates for 802.11n with 1 or 2 spatial streams.	option	-																																								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>mcs0/1</td><td>Data rate for MCS index 0 with 1 spatial stream.</td></tr><tr><td>mcs1/1</td><td>Data rate for MCS index 1 with 1 spatial stream.</td></tr><tr><td>mcs2/1</td><td>Data rate for MCS index 2 with 1 spatial stream.</td></tr><tr><td>mcs3/1</td><td>Data rate for MCS index 3 with 1 spatial stream.</td></tr><tr><td>mcs4/1</td><td>Data rate for MCS index 4 with 1 spatial stream.</td></tr><tr><td>mcs5/1</td><td>Data rate for MCS index 5 with 1 spatial stream.</td></tr><tr><td>mcs6/1</td><td>Data rate for MCS index 6 with 1 spatial stream.</td></tr></table>	Option	Description	mcs0/1	Data rate for MCS index 0 with 1 spatial stream.	mcs1/1	Data rate for MCS index 1 with 1 spatial stream.	mcs2/1	Data rate for MCS index 2 with 1 spatial stream.	mcs3/1	Data rate for MCS index 3 with 1 spatial stream.	mcs4/1	Data rate for MCS index 4 with 1 spatial stream.	mcs5/1	Data rate for MCS index 5 with 1 spatial stream.	mcs6/1	Data rate for MCS index 6 with 1 spatial stream.																										
	Option	Description																																									
	mcs0/1	Data rate for MCS index 0 with 1 spatial stream.																																									
	mcs1/1	Data rate for MCS index 1 with 1 spatial stream.																																									
	mcs2/1	Data rate for MCS index 2 with 1 spatial stream.																																									
	mcs3/1	Data rate for MCS index 3 with 1 spatial stream.																																									
	mcs4/1	Data rate for MCS index 4 with 1 spatial stream.																																									
mcs5/1	Data rate for MCS index 5 with 1 spatial stream.																																										
mcs6/1	Data rate for MCS index 6 with 1 spatial stream.																																										

Parameter	Description	Type	Size	Default																																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>mcs7/1</i></td><td>Data rate for MCS index 7 with 1 spatial stream.</td></tr><tr><td><i>mcs8/2</i></td><td>Data rate for MCS index 8 with 2 spatial streams.</td></tr><tr><td><i>mcs9/2</i></td><td>Data rate for MCS index 9 with 2 spatial streams.</td></tr><tr><td><i>mcs10/2</i></td><td>Data rate for MCS index 10 with 2 spatial streams.</td></tr><tr><td><i>mcs11/2</i></td><td>Data rate for MCS index 11 with 2 spatial streams.</td></tr><tr><td><i>mcs12/2</i></td><td>Data rate for MCS index 12 with 2 spatial streams.</td></tr><tr><td><i>mcs13/2</i></td><td>Data rate for MCS index 13 with 2 spatial streams.</td></tr><tr><td><i>mcs14/2</i></td><td>Data rate for MCS index 14 with 2 spatial streams.</td></tr><tr><td><i>mcs15/2</i></td><td>Data rate for MCS index 15 with 2 spatial streams.</td></tr></table>	Option	Description	<i>mcs7/1</i>	Data rate for MCS index 7 with 1 spatial stream.	<i>mcs8/2</i>	Data rate for MCS index 8 with 2 spatial streams.	<i>mcs9/2</i>	Data rate for MCS index 9 with 2 spatial streams.	<i>mcs10/2</i>	Data rate for MCS index 10 with 2 spatial streams.	<i>mcs11/2</i>	Data rate for MCS index 11 with 2 spatial streams.	<i>mcs12/2</i>	Data rate for MCS index 12 with 2 spatial streams.	<i>mcs13/2</i>	Data rate for MCS index 13 with 2 spatial streams.	<i>mcs14/2</i>	Data rate for MCS index 14 with 2 spatial streams.	<i>mcs15/2</i>	Data rate for MCS index 15 with 2 spatial streams.																	
	Option	Description																																				
	<i>mcs7/1</i>	Data rate for MCS index 7 with 1 spatial stream.																																				
	<i>mcs8/2</i>	Data rate for MCS index 8 with 2 spatial streams.																																				
	<i>mcs9/2</i>	Data rate for MCS index 9 with 2 spatial streams.																																				
	<i>mcs10/2</i>	Data rate for MCS index 10 with 2 spatial streams.																																				
	<i>mcs11/2</i>	Data rate for MCS index 11 with 2 spatial streams.																																				
	<i>mcs12/2</i>	Data rate for MCS index 12 with 2 spatial streams.																																				
	<i>mcs13/2</i>	Data rate for MCS index 13 with 2 spatial streams.																																				
	<i>mcs14/2</i>	Data rate for MCS index 14 with 2 spatial streams.																																				
<i>mcs15/2</i>	Data rate for MCS index 15 with 2 spatial streams.																																					
rates-11n-ss34	Allowed data rates for 802.11n with 3 or 4 spatial streams.	option	-																																			
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>mcs16/3</i></td><td>Data rate for MCS index 16 with 3 spatial streams.</td></tr><tr><td><i>mcs17/3</i></td><td>Data rate for MCS index 17 with 3 spatial streams.</td></tr><tr><td><i>mcs18/3</i></td><td>Data rate for MCS index 18 with 3 spatial streams.</td></tr><tr><td><i>mcs19/3</i></td><td>Data rate for MCS index 19 with 3 spatial streams.</td></tr><tr><td><i>mcs20/3</i></td><td>Data rate for MCS index 20 with 3 spatial streams.</td></tr><tr><td><i>mcs21/3</i></td><td>Data rate for MCS index 21 with 3 spatial streams.</td></tr><tr><td><i>mcs22/3</i></td><td>Data rate for MCS index 22 with 3 spatial streams.</td></tr><tr><td><i>mcs23/3</i></td><td>Data rate for MCS index 23 with 3 spatial streams.</td></tr><tr><td><i>mcs24/4</i></td><td>Data rate for MCS index 24 with 4 spatial streams.</td></tr><tr><td><i>mcs25/4</i></td><td>Data rate for MCS index 25 with 4 spatial streams.</td></tr><tr><td><i>mcs26/4</i></td><td>Data rate for MCS index 26 with 4 spatial streams.</td></tr><tr><td><i>mcs27/4</i></td><td>Data rate for MCS index 27 with 4 spatial streams.</td></tr><tr><td><i>mcs28/4</i></td><td>Data rate for MCS index 28 with 4 spatial streams.</td></tr><tr><td><i>mcs29/4</i></td><td>Data rate for MCS index 29 with 4 spatial streams.</td></tr><tr><td><i>mcs30/4</i></td><td>Data rate for MCS index 30 with 4 spatial streams.</td></tr><tr><td><i>mcs31/4</i></td><td>Data rate for MCS index 31 with 4 spatial streams.</td></tr></table>	Option	Description	<i>mcs16/3</i>	Data rate for MCS index 16 with 3 spatial streams.	<i>mcs17/3</i>	Data rate for MCS index 17 with 3 spatial streams.	<i>mcs18/3</i>	Data rate for MCS index 18 with 3 spatial streams.	<i>mcs19/3</i>	Data rate for MCS index 19 with 3 spatial streams.	<i>mcs20/3</i>	Data rate for MCS index 20 with 3 spatial streams.	<i>mcs21/3</i>	Data rate for MCS index 21 with 3 spatial streams.	<i>mcs22/3</i>	Data rate for MCS index 22 with 3 spatial streams.	<i>mcs23/3</i>	Data rate for MCS index 23 with 3 spatial streams.	<i>mcs24/4</i>	Data rate for MCS index 24 with 4 spatial streams.	<i>mcs25/4</i>	Data rate for MCS index 25 with 4 spatial streams.	<i>mcs26/4</i>	Data rate for MCS index 26 with 4 spatial streams.	<i>mcs27/4</i>	Data rate for MCS index 27 with 4 spatial streams.	<i>mcs28/4</i>	Data rate for MCS index 28 with 4 spatial streams.	<i>mcs29/4</i>	Data rate for MCS index 29 with 4 spatial streams.	<i>mcs30/4</i>	Data rate for MCS index 30 with 4 spatial streams.	<i>mcs31/4</i>	Data rate for MCS index 31 with 4 spatial streams.			
	Option	Description																																				
	<i>mcs16/3</i>	Data rate for MCS index 16 with 3 spatial streams.																																				
	<i>mcs17/3</i>	Data rate for MCS index 17 with 3 spatial streams.																																				
	<i>mcs18/3</i>	Data rate for MCS index 18 with 3 spatial streams.																																				
	<i>mcs19/3</i>	Data rate for MCS index 19 with 3 spatial streams.																																				
	<i>mcs20/3</i>	Data rate for MCS index 20 with 3 spatial streams.																																				
	<i>mcs21/3</i>	Data rate for MCS index 21 with 3 spatial streams.																																				
	<i>mcs22/3</i>	Data rate for MCS index 22 with 3 spatial streams.																																				
	<i>mcs23/3</i>	Data rate for MCS index 23 with 3 spatial streams.																																				
	<i>mcs24/4</i>	Data rate for MCS index 24 with 4 spatial streams.																																				
	<i>mcs25/4</i>	Data rate for MCS index 25 with 4 spatial streams.																																				
	<i>mcs26/4</i>	Data rate for MCS index 26 with 4 spatial streams.																																				
	<i>mcs27/4</i>	Data rate for MCS index 27 with 4 spatial streams.																																				
	<i>mcs28/4</i>	Data rate for MCS index 28 with 4 spatial streams.																																				
	<i>mcs29/4</i>	Data rate for MCS index 29 with 4 spatial streams.																																				
<i>mcs30/4</i>	Data rate for MCS index 30 with 4 spatial streams.																																					
<i>mcs31/4</i>	Data rate for MCS index 31 with 4 spatial streams.																																					
sae-groups	SAE-Groups.	option	-																																			

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>19</td><td>DH Group 19.</td></tr><tr><td>20</td><td>DH Group 20.</td></tr><tr><td>21</td><td>DH Group 21.</td></tr></table>	Option	Description	19	DH Group 19.	20	DH Group 20.	21	DH Group 21.			
	Option	Description										
	19	DH Group 19.										
	20	DH Group 20.										
21	DH Group 21.											
sae-h2e-only	Use hash-to-element-only mechanism for PWE derivation.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable WAP3 SAE-H2E-only.</td></tr><tr><td>disable</td><td>Disable WPA3 SAE-H2E-only.</td></tr></table>	Option	Description	enable	Enable WAP3 SAE-H2E-only.	disable	Disable WPA3 SAE-H2E-only.					
	Option	Description										
	enable	Enable WAP3 SAE-H2E-only.										
disable	Disable WPA3 SAE-H2E-only.											
sae-password	WPA3 SAE password to be used to authenticate WiFi users.	password	Not Specified									
sae-pk	Enable/disable WPA3 SAE-PK.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable WAP3 SAE-PK.</td></tr><tr><td>disable</td><td>Disable WPA3 SAE-PK.</td></tr></table>	Option	Description	enable	Enable WAP3 SAE-PK.	disable	Disable WPA3 SAE-PK.					
	Option	Description										
	enable	Enable WAP3 SAE-PK.										
disable	Disable WPA3 SAE-PK.											
sae-private-key	Private key used for WPA3 SAE-PK authentication.	string	Maximum length: 359									
scan-botnet-connections	Block or monitor connections to Botnet servers or disable Botnet scanning.	option	-	monitor								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Do not scan connections to botnet servers.</td></tr><tr><td>monitor</td><td>Log connections to botnet servers.</td></tr><tr><td>block</td><td>Block connections to botnet servers.</td></tr></table>	Option	Description	disable	Do not scan connections to botnet servers.	monitor	Log connections to botnet servers.	block	Block connections to botnet servers.			
	Option	Description										
	disable	Do not scan connections to botnet servers.										
	monitor	Log connections to botnet servers.										
block	Block connections to botnet servers.											
schedule <name>	Firewall schedules for enabling this VAP on the FortiAP. This VAP will be enabled when at least one of the schedules is valid. Separate multiple schedule names with a space. Schedule name.	string	Maximum length: 35									
secondary-wag-profile	Secondary wireless access gateway profile name.	string	Maximum length: 35									
security	Security mode for the wireless interface.	option	-	wpa2-only-personal								

Parameter	Description	Type	Size	Default																																											
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>open</i></td><td>Open.</td></tr><tr><td><i>captive-portal</i></td><td>Captive portal.</td></tr><tr><td><i>wep64</i></td><td>WEP 64-bit.</td></tr><tr><td><i>wep128</i></td><td>WEP 128-bit.</td></tr><tr><td><i>wpa-personal</i></td><td>WPA/WPA2 personal.</td></tr><tr><td><i>wpa-personal+captive-portal</i></td><td>WPA/WPA2 personal with captive portal.</td></tr><tr><td><i>wpa-enterprise</i></td><td>WPA/WPA2 enterprise.</td></tr><tr><td><i>wpa-only-personal</i></td><td>WPA personal.</td></tr><tr><td><i>wpa-only-personal+captive-portal</i></td><td>WPA personal with captive portal.</td></tr><tr><td><i>wpa-only-enterprise</i></td><td>WPA enterprise.</td></tr><tr><td><i>wpa2-only-personal</i></td><td>WPA2 personal.</td></tr><tr><td><i>wpa2-only-personal+captive-portal</i></td><td>WPA2 personal with captive portal.</td></tr><tr><td><i>wpa2-only-enterprise</i></td><td>WPA2 enterprise.</td></tr><tr><td><i>wpa3-enterprise</i></td><td>WPA3 enterprise with 192-bit encryption and PMF mandatory.</td></tr><tr><td><i>wpa3-only-enterprise</i></td><td>WPA3 enterprise with PMF mandatory.</td></tr><tr><td><i>wpa3-enterprise-transition</i></td><td>WPA3 enterprise with PMF optional.</td></tr><tr><td><i>wpa3-sae</i></td><td>WPA3 SAE.</td></tr><tr><td><i>wpa3-sae-transition</i></td><td>WPA3 SAE transition.</td></tr><tr><td><i>owe</i></td><td>Opportunistic wireless encryption.</td></tr><tr><td><i>osen</i></td><td>OSEN.</td></tr></table>	Option	Description	<i>open</i>	Open.	<i>captive-portal</i>	Captive portal.	<i>wep64</i>	WEP 64-bit.	<i>wep128</i>	WEP 128-bit.	<i>wpa-personal</i>	WPA/WPA2 personal.	<i>wpa-personal+captive-portal</i>	WPA/WPA2 personal with captive portal.	<i>wpa-enterprise</i>	WPA/WPA2 enterprise.	<i>wpa-only-personal</i>	WPA personal.	<i>wpa-only-personal+captive-portal</i>	WPA personal with captive portal.	<i>wpa-only-enterprise</i>	WPA enterprise.	<i>wpa2-only-personal</i>	WPA2 personal.	<i>wpa2-only-personal+captive-portal</i>	WPA2 personal with captive portal.	<i>wpa2-only-enterprise</i>	WPA2 enterprise.	<i>wpa3-enterprise</i>	WPA3 enterprise with 192-bit encryption and PMF mandatory.	<i>wpa3-only-enterprise</i>	WPA3 enterprise with PMF mandatory.	<i>wpa3-enterprise-transition</i>	WPA3 enterprise with PMF optional.	<i>wpa3-sae</i>	WPA3 SAE.	<i>wpa3-sae-transition</i>	WPA3 SAE transition.	<i>owe</i>	Opportunistic wireless encryption.	<i>osen</i>	OSEN.				
	Option	Description																																													
	<i>open</i>	Open.																																													
	<i>captive-portal</i>	Captive portal.																																													
	<i>wep64</i>	WEP 64-bit.																																													
	<i>wep128</i>	WEP 128-bit.																																													
	<i>wpa-personal</i>	WPA/WPA2 personal.																																													
	<i>wpa-personal+captive-portal</i>	WPA/WPA2 personal with captive portal.																																													
	<i>wpa-enterprise</i>	WPA/WPA2 enterprise.																																													
	<i>wpa-only-personal</i>	WPA personal.																																													
	<i>wpa-only-personal+captive-portal</i>	WPA personal with captive portal.																																													
	<i>wpa-only-enterprise</i>	WPA enterprise.																																													
	<i>wpa2-only-personal</i>	WPA2 personal.																																													
	<i>wpa2-only-personal+captive-portal</i>	WPA2 personal with captive portal.																																													
	<i>wpa2-only-enterprise</i>	WPA2 enterprise.																																													
	<i>wpa3-enterprise</i>	WPA3 enterprise with 192-bit encryption and PMF mandatory.																																													
	<i>wpa3-only-enterprise</i>	WPA3 enterprise with PMF mandatory.																																													
	<i>wpa3-enterprise-transition</i>	WPA3 enterprise with PMF optional.																																													
	<i>wpa3-sae</i>	WPA3 SAE.																																													
	<i>wpa3-sae-transition</i>	WPA3 SAE transition.																																													
<i>owe</i>	Opportunistic wireless encryption.																																														
<i>osen</i>	OSEN.																																														
security-exempt-list	Optional security exempt list for captive portal authentication.	string	Maximum length: 35																																												
security-redirect-url	Optional URL for redirecting users after they pass captive portal authentication.	var-string	Maximum length: 1023																																												

Parameter	Description	Type	Size	Default						
selected-usergroups <name>	Selective user groups that are permitted to authenticate. User group name.	string	Maximum length: 79							
split-tunneling	Enable/disable split tunneling.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable split tunneling.</td></tr><tr><td>disable</td><td>Disable split tunneling.</td></tr></table>	Option	Description	enable	Enable split tunneling.	disable	Disable split tunneling.			
Option	Description									
enable	Enable split tunneling.									
disable	Disable split tunneling.									
ssid	IEEE 802.11 service set identifier (SSID) for the wireless interface. Users who wish to use the wireless network must configure their computers to access this SSID name.	string	Maximum length: 32	fortinet						
sticky-client-remove	Enable/disable sticky client remove to maintain good signal level clients in SSID.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable sticky client remove.</td></tr><tr><td>disable</td><td>Disable sticky client remove.</td></tr></table>	Option	Description	enable	Enable sticky client remove.	disable	Disable sticky client remove.			
Option	Description									
enable	Enable sticky client remove.									
disable	Disable sticky client remove.									
sticky-client-threshold-2g	Minimum signal level/threshold in dBm required for the 2G client to be serviced by the AP.	string	Maximum length: 7	-79						
sticky-client-threshold-5g	Minimum signal level/threshold in dBm required for the 5G client to be serviced by the AP.	string	Maximum length: 7	-76						
sticky-client-threshold-6g	Minimum signal level/threshold in dBm required for the 6G client to be serviced by the AP.	string	Maximum length: 7	-76						
target-wake-time	Enable/disable 802.11ax target wake time.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable 802.11ax target wake time.</td></tr><tr><td>disable</td><td>Disable 802.11ax target wake time.</td></tr></table>	Option	Description	enable	Enable 802.11ax target wake time.	disable	Disable 802.11ax target wake time.			
Option	Description									
enable	Enable 802.11ax target wake time.									
disable	Disable 802.11ax target wake time.									
tkip-counter-measure	Enable/disable TKIP counter measure.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable TKIP counter measure.</td></tr></table>	Option	Description	enable	Enable TKIP counter measure.					
Option	Description									
enable	Enable TKIP counter measure.									



Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable TKIP counter measure.</td></tr></table>	Option	Description	<i>disable</i>	Disable TKIP counter measure.					
Option	Description									
<i>disable</i>	Disable TKIP counter measure.									
tunnel-echo-interval	The time interval to send echo to both primary and secondary tunnel peers.	integer	Minimum value: 1 Maximum value: 65535	300						
tunnel-fallback-interval	The time interval for secondary tunnel to fall back to primary tunnel.	integer	Minimum value: 0 Maximum value: 65535	7200						
usergroup <name>	Firewall user group to be used to authenticate WiFi users. User group name.	string	Maximum length: 79							
utm-log	Enable/disable UTM logging.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable UTM logging.</td></tr><tr><td><i>disable</i></td><td>Disable UTM logging.</td></tr></table>	Option	Description	<i>enable</i>	Enable UTM logging.	<i>disable</i>	Disable UTM logging.			
Option	Description									
<i>enable</i>	Enable UTM logging.									
<i>disable</i>	Disable UTM logging.									
utm-profile	UTM profile name.	string	Maximum length: 35							
utm-status	Enable to add one or more security profiles (AV, IPS, etc.) to the VAP.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable setting.</td></tr><tr><td><i>disable</i></td><td>Disable setting.</td></tr></table>	Option	Description	<i>enable</i>	Enable setting.	<i>disable</i>	Disable setting.			
Option	Description									
<i>enable</i>	Enable setting.									
<i>disable</i>	Disable setting.									
vlan-auto	Enable/disable automatic management of SSID VLAN interface.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable automatic management of SSID VLAN interface.</td></tr><tr><td><i>disable</i></td><td>Disable automatic management of SSID VLAN interface.</td></tr></table>	Option	Description	<i>enable</i>	Enable automatic management of SSID VLAN interface.	<i>disable</i>	Disable automatic management of SSID VLAN interface.			
Option	Description									
<i>enable</i>	Enable automatic management of SSID VLAN interface.									
<i>disable</i>	Disable automatic management of SSID VLAN interface.									
vlan-pooling	Enable/disable VLAN pooling, to allow grouping of multiple wireless controller VLANs into VLAN pools. When set to wtp-group, VLAN pooling occurs with VLAN assignment by wtp-group.	option	-	disable						

Parameter	Description	Type	Size	Default										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>wtp-group</i></td><td>Enable VLAN pooling with VLAN assignment by wtp-group.</td></tr><tr><td><i>round-robin</i></td><td>Enable VLAN pooling with round-robin VLAN assignment.</td></tr><tr><td><i>hash</i></td><td>Enable VLAN pooling with hash-based VLAN assignment.</td></tr><tr><td><i>disable</i></td><td>Disable VLAN pooling.</td></tr></table>	Option	Description	<i>wtp-group</i>	Enable VLAN pooling with VLAN assignment by wtp-group.	<i>round-robin</i>	Enable VLAN pooling with round-robin VLAN assignment.	<i>hash</i>	Enable VLAN pooling with hash-based VLAN assignment.	<i>disable</i>	Disable VLAN pooling.			
	Option	Description												
	<i>wtp-group</i>	Enable VLAN pooling with VLAN assignment by wtp-group.												
	<i>round-robin</i>	Enable VLAN pooling with round-robin VLAN assignment.												
	<i>hash</i>	Enable VLAN pooling with hash-based VLAN assignment.												
<i>disable</i>	Disable VLAN pooling.													
vlanid	Optional VLAN ID.	integer	Minimum value: 0 Maximum value: 4094	0										
voice-enterprise	Enable/disable 802.11k and 802.11v assisted Voice-Enterprise roaming.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable 802.11k and 802.11v assisted Voice-Enterprise roaming.</td></tr><tr><td><i>enable</i></td><td>Enable 802.11k and 802.11v assisted Voice-Enterprise roaming.</td></tr></table>	Option	Description	<i>disable</i>	Disable 802.11k and 802.11v assisted Voice-Enterprise roaming.	<i>enable</i>	Enable 802.11k and 802.11v assisted Voice-Enterprise roaming.							
	Option	Description												
	<i>disable</i>	Disable 802.11k and 802.11v assisted Voice-Enterprise roaming.												
<i>enable</i>	Enable 802.11k and 802.11v assisted Voice-Enterprise roaming.													
webfilter-profile	WebFilter profile name.	string	Maximum length: 35											

### config mac-filter-list

Parameter	Description	Type	Size	Default						
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0						
mac	MAC address.	mac-address	Not Specified	00:00:00:00:00:00						
mac-filter-policy	Deny or allow the client with this MAC address.	option	-	deny						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>allow</i></td><td>Allow the client with this MAC address.</td></tr><tr><td><i>deny</i></td><td>Block the client with this MAC address.</td></tr></table>				Option	Description	<i>allow</i>	Allow the client with this MAC address.	<i>deny</i>	Block the client with this MAC address.
Option	Description									
<i>allow</i>	Allow the client with this MAC address.									
<i>deny</i>	Block the client with this MAC address.									

## config portal-message-overrides

Parameter	Description	Type	Size	Default
auth-disclaimer-page	Override auth-disclaimer-page message with message from portal-message-overrides group.	string	Maximum length: 35	
auth-reject-page	Override auth-reject-page message with message from portal-message-overrides group.	string	Maximum length: 35	
auth-login-page	Override auth-login-page message with message from portal-message-overrides group.	string	Maximum length: 35	
auth-login-failed-page	Override auth-login-failed-page message with message from portal-message-overrides group.	string	Maximum length: 35	

## config vlan-name

Parameter	Description	Type	Size	Default
name	VLAN name.	string	Maximum length: 35	
vlan-id	VLAN ID.	integer	Minimum value: 0 Maximum value: 4094	0

## config vlan-pool

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4094	0
wtp-group	WTP group name.	string	Maximum length: 35	

## config wireless-controller wag-profile

Configure wireless access gateway (WAG) profiles used for tunnels on AP.

```
config wireless-controller wag-profile
  Description: Configure wireless access gateway (WAG) profiles used for tunnels on AP.
  edit <name>
    set comment {var-string}
    set dhcp-ip-addr {ipv4-address}
    set ping-interval {integer}
    set ping-number {integer}
```

```

        set return-packet-timeout {integer}
        set tunnel-type [l2tpv3|gre]
        set wag-ip {ipv4-address}
        set wag-port {integer}
    next
end

```

## config wireless-controller wag-profile

Parameter	Description	Type	Size	Default						
comment	Comment.	var-string	Maximum length: 255							
dhcp-ip-addr	IP address of the monitoring DHCP request packet sent through the tunnel.	ipv4-address	Not Specified	0.0.0.0						
name	Tunnel profile name.	string	Maximum length: 35							
ping-interval	Interval between two tunnel monitoring echo packets.	integer	Minimum value: 1 Maximum value: 65535	1						
ping-number	Number of the tunnel monitoring echo packets.	integer	Minimum value: 1 Maximum value: 65535	5						
return-packet-timeout	Window of time for the return packets from the tunnel's remote end.	integer	Minimum value: 1 Maximum value: 65535	160						
tunnel-type	Tunnel type.	option	-	l2tpv3						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>l2tpv3</i></td><td>L2TPV3 Ethernet Pseudowire.</td></tr><tr><td><i>gre</i></td><td>GRE Ethernet tunnel.</td></tr></table>				Option	Description	<i>l2tpv3</i>	L2TPV3 Ethernet Pseudowire.	<i>gre</i>	GRE Ethernet tunnel.
Option	Description									
<i>l2tpv3</i>	L2TPV3 Ethernet Pseudowire.									
<i>gre</i>	GRE Ethernet tunnel.									
wag-ip	IP Address of the wireless access gateway.	ipv4-address	Not Specified	0.0.0.0						
wag-port	UDP port of the wireless access gateway.	integer	Minimum value: 0 Maximum value: 65535	1701						

---

## config wireless-controller wids-profile

Configure wireless intrusion detection system (WIDS) profiles.

```
config wireless-controller wids-profile
  Description: Configure wireless intrusion detection system (WIDS) profiles.
  edit <name>
    set ap-auto-suppress [enable|disable]
    set ap-bgscan-disable-schedules <name1>, <name2>, ...
    set ap-bgscan-duration {integer}
    set ap-bgscan-idle {integer}
    set ap-bgscan-intv {integer}
    set ap-bgscan-period {integer}
    set ap-bgscan-report-intv {integer}
    set ap-fgscan-report-intv {integer}
    set ap-scan [disable|enable]
    set ap-scan-passive [enable|disable]
    set ap-scan-threshold {string}
    set asleap-attack [enable|disable]
    set assoc-flood-thresh {integer}
    set assoc-flood-time {integer}
    set assoc-frame-flood [enable|disable]
    set auth-flood-thresh {integer}
    set auth-flood-time {integer}
    set auth-frame-flood [enable|disable]
    set comment {string}
    set deauth-broadcast [enable|disable]
    set deauth-unknown-src-thresh {integer}
    set eapol-fail-flood [enable|disable]
    set eapol-fail-intv {integer}
    set eapol-fail-thresh {integer}
    set eapol-logoff-flood [enable|disable]
    set eapol-logoff-intv {integer}
    set eapol-logoff-thresh {integer}
    set eapol-pre-fail-flood [enable|disable]
    set eapol-pre-fail-intv {integer}
    set eapol-pre-fail-thresh {integer}
    set eapol-pre-succ-flood [enable|disable]
    set eapol-pre-succ-intv {integer}
    set eapol-pre-succ-thresh {integer}
    set eapol-start-flood [enable|disable]
    set eapol-start-intv {integer}
    set eapol-start-thresh {integer}
    set eapol-succ-flood [enable|disable]
    set eapol-succ-intv {integer}
    set eapol-succ-thresh {integer}
    set invalid-mac-oui [enable|disable]
    set long-duration-attack [enable|disable]
    set long-duration-thresh {integer}
    set null-ssid-probe-resp [enable|disable]
    set sensor-mode [disable|foreign|...]
    set spoofed-deauth [enable|disable]
    set weak-wep-iv [enable|disable]
    set wireless-bridge [enable|disable]
  next
end
```

## config wireless-controller wids-profile

Parameter	Description	Type	Size	Default
ap-auto-suppress	Enable/disable on-wire rogue AP auto-suppression.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable on-wire rogue AP auto-suppression.		
	<i>disable</i>	Disable on-wire rogue AP auto-suppression.		
ap-bgscan-disable-schedules <name>	Firewall schedules for turning off FortiAP radio background scan. Background scan will be disabled when at least one of the schedules is valid. Separate multiple schedule names with a space. Schedule name.	string	Maximum length: 35	
ap-bgscan-duration	Listen time on scanning a channel.	integer	Minimum value: 10 Maximum value: 1000	30
ap-bgscan-idle	Wait time for channel inactivity before scanning this channel.	integer	Minimum value: 0 Maximum value: 1000	20
ap-bgscan-intv	Period between successive channel scans.	integer	Minimum value: 1 Maximum value: 600	3
ap-bgscan-period	Period between background scans.	integer	Minimum value: 10 Maximum value: 3600	600
ap-bgscan-report-intv	Period between background scan reports.	integer	Minimum value: 15 Maximum value: 600	30
ap-fgscan-report-intv	Period between foreground scan reports.	integer	Minimum value: 15 Maximum value: 600	15
ap-scan	Enable/disable rogue AP detection.	option	-	disable

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable rogue AP detection.		
	<i>enable</i>	Enable rogue AP detection.		
ap-scan-passive	Enable/disable passive scanning. Enable means do not send probe request on any channels.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Passive scanning on all channels.		
	<i>disable</i>	Passive scanning only on DFS channels.		
ap-scan-threshold	Minimum signal level/threshold in dBm required for the AP to report detected rogue AP.	string	Maximum length: 7	-90
asleep-attack	Enable/disable asleep attack detection.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable asleep attack detection.		
	<i>disable</i>	Disable asleep attack detection.		
assoc-flood-thresh	The threshold value for association frame flooding.	integer	Minimum value: 1 Maximum value: 100	30
assoc-flood-time	Number of seconds after which a station is considered not connected.	integer	Minimum value: 5 Maximum value: 120	10
assoc-frame-flood	Enable/disable association frame flooding detection.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable association frame flooding detection.		
	<i>disable</i>	Disable association frame flooding detection.		
auth-flood-thresh	The threshold value for authentication frame flooding.	integer	Minimum value: 1 Maximum value: 100	30

Parameter	Description	Type	Size	Default						
auth-flood-time	Number of seconds after which a station is considered not connected.	integer	Minimum value: 5 Maximum value: 120	10						
auth-frame-flood	Enable/disable authentication frame flooding detection.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable authentication frame flooding detection.</td></tr><tr><td><i>disable</i></td><td>Disable authentication frame flooding detection.</td></tr></table>	Option	Description	<i>enable</i>	Enable authentication frame flooding detection.	<i>disable</i>	Disable authentication frame flooding detection.			
Option	Description									
<i>enable</i>	Enable authentication frame flooding detection.									
<i>disable</i>	Disable authentication frame flooding detection.									
comment	Comment.	string	Maximum length: 63							
deauth-broadcast	Enable/disable broadcasting de-authentication detection.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable broadcast de-authentication detection.</td></tr><tr><td><i>disable</i></td><td>Disable broadcast de-authentication detection.</td></tr></table>	Option	Description	<i>enable</i>	Enable broadcast de-authentication detection.	<i>disable</i>	Disable broadcast de-authentication detection.			
Option	Description									
<i>enable</i>	Enable broadcast de-authentication detection.									
<i>disable</i>	Disable broadcast de-authentication detection.									
deauth-unknown-src-thresh	Threshold value per second to deauth unknown src for DoS attack (0: no limit).	integer	Minimum value: 0 Maximum value: 65535	10						
eapol-fail-flood	Enable/disable EAPOL-Failure flooding.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable EAPOL-Failure flooding detection.</td></tr><tr><td><i>disable</i></td><td>Disable EAPOL-Failure flooding detection.</td></tr></table>	Option	Description	<i>enable</i>	Enable EAPOL-Failure flooding detection.	<i>disable</i>	Disable EAPOL-Failure flooding detection.			
Option	Description									
<i>enable</i>	Enable EAPOL-Failure flooding detection.									
<i>disable</i>	Disable EAPOL-Failure flooding detection.									
eapol-fail-intv	The detection interval for EAPOL-Failure flooding.	integer	Minimum value: 1 Maximum value: 3600	1						
eapol-fail-thresh	The threshold value for EAPOL-Failure flooding in specified interval.	integer	Minimum value: 2 Maximum value: 100	10						



Parameter	Description	Type	Size	Default						
eapol-logoff-flood	Enable/disable EAPOL-Logoff flooding.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable EAPOL-Logoff flooding detection.</td></tr><tr><td><i>disable</i></td><td>Disable EAPOL-Logoff flooding detection.</td></tr></table>	Option	Description	<i>enable</i>	Enable EAPOL-Logoff flooding detection.	<i>disable</i>	Disable EAPOL-Logoff flooding detection.			
Option	Description									
<i>enable</i>	Enable EAPOL-Logoff flooding detection.									
<i>disable</i>	Disable EAPOL-Logoff flooding detection.									
eapol-logoff-intv	The detection interval for EAPOL-Logoff flooding.	integer	Minimum value: 1 Maximum value: 3600	1						
eapol-logoff-thresh	The threshold value for EAPOL-Logoff flooding in specified interval.	integer	Minimum value: 2 Maximum value: 100	10						
eapol-pre-fail-flood	Enable/disable premature EAPOL-Failure flooding.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable premature EAPOL-Failure flooding detection.</td></tr><tr><td><i>disable</i></td><td>Disable premature EAPOL-Failure flooding detection.</td></tr></table>	Option	Description	<i>enable</i>	Enable premature EAPOL-Failure flooding detection.	<i>disable</i>	Disable premature EAPOL-Failure flooding detection.			
Option	Description									
<i>enable</i>	Enable premature EAPOL-Failure flooding detection.									
<i>disable</i>	Disable premature EAPOL-Failure flooding detection.									
eapol-pre-fail-intv	The detection interval for premature EAPOL-Failure flooding.	integer	Minimum value: 1 Maximum value: 3600	1						
eapol-pre-fail-thresh	The threshold value for premature EAPOL-Failure flooding in specified interval.	integer	Minimum value: 2 Maximum value: 100	10						
eapol-pre-succ-flood	Enable/disable premature EAPOL-Success flooding.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable premature EAPOL-Success flooding detection.</td></tr><tr><td><i>disable</i></td><td>Disable premature EAPOL-Success flooding detection.</td></tr></table>	Option	Description	<i>enable</i>	Enable premature EAPOL-Success flooding detection.	<i>disable</i>	Disable premature EAPOL-Success flooding detection.			
Option	Description									
<i>enable</i>	Enable premature EAPOL-Success flooding detection.									
<i>disable</i>	Disable premature EAPOL-Success flooding detection.									
eapol-pre-succ-intv	The detection interval for premature EAPOL-Success flooding.	integer	Minimum value: 1 Maximum value: 3600	1						

Parameter	Description	Type	Size	Default						
eapol-pre-succ-thresh	The threshold value for premature EAPOL-Success flooding in specified interval.	integer	Minimum value: 2 Maximum value: 100	10						
eapol-start-flood	Enable/disable EAPOL-Start flooding.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable EAPOL-Start flooding detection.</td></tr><tr><td><i>disable</i></td><td>Disable EAPOL-Start flooding detection.</td></tr></table>	Option	Description	<i>enable</i>	Enable EAPOL-Start flooding detection.	<i>disable</i>	Disable EAPOL-Start flooding detection.			
Option	Description									
<i>enable</i>	Enable EAPOL-Start flooding detection.									
<i>disable</i>	Disable EAPOL-Start flooding detection.									
eapol-start-intv	The detection interval for EAPOL-Start flooding.	integer	Minimum value: 1 Maximum value: 3600	1						
eapol-start-thresh	The threshold value for EAPOL-Start flooding in specified interval.	integer	Minimum value: 2 Maximum value: 100	10						
eapol-succ-flood	Enable/disable EAPOL-Success flooding.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable EAPOL-Success flooding detection.</td></tr><tr><td><i>disable</i></td><td>Disable EAPOL-Success flooding detection.</td></tr></table>	Option	Description	<i>enable</i>	Enable EAPOL-Success flooding detection.	<i>disable</i>	Disable EAPOL-Success flooding detection.			
Option	Description									
<i>enable</i>	Enable EAPOL-Success flooding detection.									
<i>disable</i>	Disable EAPOL-Success flooding detection.									
eapol-succ-intv	The detection interval for EAPOL-Success flooding.	integer	Minimum value: 1 Maximum value: 3600	1						
eapol-succ-thresh	The threshold value for EAPOL-Success flooding in specified interval.	integer	Minimum value: 2 Maximum value: 100	10						
invalid-mac-oui	Enable/disable invalid MAC OUI detection.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable invalid MAC OUI detection.</td></tr><tr><td><i>disable</i></td><td>Disable invalid MAC OUI detection.</td></tr></table>	Option	Description	<i>enable</i>	Enable invalid MAC OUI detection.	<i>disable</i>	Disable invalid MAC OUI detection.			
Option	Description									
<i>enable</i>	Enable invalid MAC OUI detection.									
<i>disable</i>	Disable invalid MAC OUI detection.									

Parameter	Description	Type	Size	Default								
long-duration-attack	Enable/disable long duration attack detection based on user configured threshold.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable long duration attack detection.</td></tr><tr><td><i>disable</i></td><td>Disable long duration attack detection.</td></tr></table>	Option	Description	<i>enable</i>	Enable long duration attack detection.	<i>disable</i>	Disable long duration attack detection.					
Option	Description											
<i>enable</i>	Enable long duration attack detection.											
<i>disable</i>	Disable long duration attack detection.											
long-duration-thresh	Threshold value for long duration attack detection.	integer	Minimum value: 1000 Maximum value: 32767	8200								
name	WIDS profile name.	string	Maximum length: 35									
null-ssid-probe-resp	Enable/disable null SSID probe response detection.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable null SSID probe resp detection.</td></tr><tr><td><i>disable</i></td><td>Disable null SSID probe resp detection.</td></tr></table>	Option	Description	<i>enable</i>	Enable null SSID probe resp detection.	<i>disable</i>	Disable null SSID probe resp detection.					
Option	Description											
<i>enable</i>	Enable null SSID probe resp detection.											
<i>disable</i>	Disable null SSID probe resp detection.											
sensor-mode	Scan nearby WiFi stations.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable the scan.</td></tr><tr><td><i>foreign</i></td><td>Enable the scan and monitor foreign channels. Foreign channels are all other available channels than the current operating channel.</td></tr><tr><td><i>both</i></td><td>Enable the scan and monitor both foreign and home channels. Select this option to monitor all WiFi channels.</td></tr></table>	Option	Description	<i>disable</i>	Disable the scan.	<i>foreign</i>	Enable the scan and monitor foreign channels. Foreign channels are all other available channels than the current operating channel.	<i>both</i>	Enable the scan and monitor both foreign and home channels. Select this option to monitor all WiFi channels.			
Option	Description											
<i>disable</i>	Disable the scan.											
<i>foreign</i>	Enable the scan and monitor foreign channels. Foreign channels are all other available channels than the current operating channel.											
<i>both</i>	Enable the scan and monitor both foreign and home channels. Select this option to monitor all WiFi channels.											
spoofed-deauth	Enable/disable spoofed de-authentication attack detection.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable spoofed de-authentication attack detection.</td></tr><tr><td><i>disable</i></td><td>Disable spoofed de-authentication attack detection.</td></tr></table>	Option	Description	<i>enable</i>	Enable spoofed de-authentication attack detection.	<i>disable</i>	Disable spoofed de-authentication attack detection.					
Option	Description											
<i>enable</i>	Enable spoofed de-authentication attack detection.											
<i>disable</i>	Disable spoofed de-authentication attack detection.											
weak-wep-iv	Enable/disable weak WEP IV.	option	-	disable								

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable weak WEP IV detection.		
	<i>disable</i>	Disable weak WEP IV detection.		
wireless-bridge	Enable/disable wireless bridge detection.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable wireless bridge detection.		
	<i>disable</i>	Disable wireless bridge detection.		

## config wireless-controller wtp-group

Configure WTP groups.

```
config wireless-controller wtp-group
  Description: Configure WTP groups.
  edit <name>
    set platform-type [AP-11N|220B|...]
    set wtps <wtp-id1>, <wtp-id2>, ...
  next
end
```

## config wireless-controller wtp-group

Parameter	Description	Type	Size	Default
name	WTP group name.	string	Maximum length: 35	
platform-type	FortiAP models to define the WTP group platform type.	option	-	
	<b>Option</b>	<b>Description</b>		
	<i>AP-11N</i>	Default 11n AP.		
	<i>220B</i>	FAP220B/221B.		
	<i>210B</i>	FAP210B.		
	<i>222B</i>	FAP222B.		
	<i>112B</i>	FAP112B.		
	<i>320B</i>	FAP320B.		
	<i>11C</i>	FAP11C.		

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	14C	FAP14C.		
	223B	FAP223B.		
	28C	FAP28C.		
	320C	FAP320C.		
	221C	FAP221C.		
	25D	FAP25D.		
	222C	FAP222C.		
	224D	FAP224D.		
	214B	FK214B.		
	21D	FAP21D.		
	24D	FAP24D.		
	112D	FAP112D.		
	223C	FAP223C.		
	321C	FAP321C.		
	C220C	FAPC220C.		
	C225C	FAPC225C.		
	C23JD	FAPC23JD.		
	C24JE	FAPC24JE.		
	S321C	FAPS321C.		
	S322C	FAPS322C.		
	S323C	FAPS323C.		
	S311C	FAPS311C.		
	S313C	FAPS313C.		
	S321CR	FAPS321CR.		
	S322CR	FAPS322CR.		
	S323CR	FAPS323CR.		
	S421E	FAPS421E.		
	S422E	FAPS422E.		
	S423E	FAPS423E.		

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>421E</i>	FAP421E.		
	<i>423E</i>	FAP423E.		
	<i>221E</i>	FAP221E.		
	<i>222E</i>	FAP222E.		
	<i>223E</i>	FAP223E.		
	<i>224E</i>	FAP224E.		
	<i>231E</i>	FAP231E.		
	<i>S221E</i>	FAPS221E.		
	<i>S223E</i>	FAPS223E.		
	<i>321E</i>	FAP321E.		
	<i>431F</i>	FAP431F.		
	<i>431FL</i>	FAP431FL.		
	<i>432F</i>	FAP432F.		
	<i>432FR</i>	FAP432FR.		
	<i>433F</i>	FAP433F.		
	<i>433FL</i>	FAP433FL.		
	<i>231F</i>	FAP231F.		
	<i>231FL</i>	FAP231FL.		
	<i>234F</i>	FAP234F.		
	<i>23JF</i>	FAP23JF.		
	<i>831F</i>	FAP831F.		
	<i>231G</i>	FAP231G.		
	<i>233G</i>	FAP233G.		
	<i>431G</i>	FAP431G.		
	<i>433G</i>	FAP433G.		
	<i>U421E</i>	FAPU421EV.		
	<i>U422EV</i>	FAPU422EV.		
	<i>U423E</i>	FAPU423EV.		
	<i>U221EV</i>	FAPU221EV.		

Parameter	Description	Type	Size	Default																								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>U223EV</i></td><td>FAPU223EV.</td></tr><tr><td><i>U24JEV</i></td><td>FAPU24JEV.</td></tr><tr><td><i>U321EV</i></td><td>FAPU321EV.</td></tr><tr><td><i>U323EV</i></td><td>FAPU323EV.</td></tr><tr><td><i>U431F</i></td><td>FAPU431F.</td></tr><tr><td><i>U433F</i></td><td>FAPU433F.</td></tr><tr><td><i>U231F</i></td><td>FAPU231F.</td></tr><tr><td><i>U234F</i></td><td>FAPU234F.</td></tr><tr><td><i>U432F</i></td><td>FAPU432F.</td></tr><tr><td><i>U231G</i></td><td>FAPU231G.</td></tr><tr><td><i>U441G</i></td><td>FAPU441G.</td></tr></table>	Option	Description	<i>U223EV</i>	FAPU223EV.	<i>U24JEV</i>	FAPU24JEV.	<i>U321EV</i>	FAPU321EV.	<i>U323EV</i>	FAPU323EV.	<i>U431F</i>	FAPU431F.	<i>U433F</i>	FAPU433F.	<i>U231F</i>	FAPU231F.	<i>U234F</i>	FAPU234F.	<i>U432F</i>	FAPU432F.	<i>U231G</i>	FAPU231G.	<i>U441G</i>	FAPU441G.			
	Option	Description																										
	<i>U223EV</i>	FAPU223EV.																										
	<i>U24JEV</i>	FAPU24JEV.																										
	<i>U321EV</i>	FAPU321EV.																										
	<i>U323EV</i>	FAPU323EV.																										
	<i>U431F</i>	FAPU431F.																										
	<i>U433F</i>	FAPU433F.																										
	<i>U231F</i>	FAPU231F.																										
	<i>U234F</i>	FAPU234F.																										
	<i>U432F</i>	FAPU432F.																										
	<i>U231G</i>	FAPU231G.																										
<i>U441G</i>	FAPU441G.																											
wtps <wtp-id>	WTP list. WTP ID.	string	Maximum length: 35																									

## config wireless-controller wtp-profile

Configure WTP profiles or FortiAP profiles that define radio settings for manageable FortiAP platforms.

```
config wireless-controller wtp-profile
```

Description: Configure WTP profiles or FortiAP profiles that define radio settings for manageable FortiAP platforms.

```
edit <name>
```

```
set allowaccess {option1}, {option2}, ...
```

```
set ap-country [--|AF|...]
```

```
set ap-handoff [enable|disable]
```

```
set apcfg-profile {string}
```

```
set ble-profile {string}
```

```
set comment {var-string}
```

```
set console-login [enable|disable]
```

```
set control-message-offload {option1}, {option2}, ...
```

```
config deny-mac-list
```

Description: List of MAC addresses that are denied access to this WTP, FortiAP,

or AP.

```
edit <id>
```

```
set mac {mac-address}
```

```
next
```

```
end
```

```
set dtls-in-kernel [enable|disable]
```

```
set dtls-policy {option1}, {option2}, ...
```

```
set energy-efficient-ethernet [enable|disable]
```

```
config esl-ses-dongle
```

Description: ESL SES-imagotag dongle configuration.

```

    set compliance-level {option}
    set scd-enable [enable|disable]
    set esl-channel [-1|0|...]
    set output-power [a|b|...]
    set apc-addr-type [fqdn|ip]
    set apc-fqdn {string}
    set apc-ip {ipv4-address}
    set apc-port {integer}
    set coex-level {option}
    set tls-cert-verification [enable|disable]
    set tls-fqdn-verification [enable|disable]
end
set ext-info-enable [enable|disable]
set frequency-handoff [enable|disable]
set handoff-roaming [enable|disable]
set handoff-rssi {integer}
set handoff-sta-thresh {integer}
set indoor-outdoor-deployment [platform-determined|outdoor|...]
set ip-fragment-preventing {option1}, {option2}, ...
config lan
    Description: WTP LAN port mapping.
    set port-mode [offline|nat-to-wan|...]
    set port-ssid {string}
    set port1-mode [offline|nat-to-wan|...]
    set port1-ssid {string}
    set port2-mode [offline|nat-to-wan|...]
    set port2-ssid {string}
    set port3-mode [offline|nat-to-wan|...]
    set port3-ssid {string}
    set port4-mode [offline|nat-to-wan|...]
    set port4-ssid {string}
    set port5-mode [offline|nat-to-wan|...]
    set port5-ssid {string}
    set port6-mode [offline|nat-to-wan|...]
    set port6-ssid {string}
    set port7-mode [offline|nat-to-wan|...]
    set port7-ssid {string}
    set port8-mode [offline|nat-to-wan|...]
    set port8-ssid {string}
    set port-esl-mode [offline|nat-to-wan|...]
    set port-esl-ssid {string}
end
config lbs
    Description: Set various location based service (LBS) options.
    set ekahau-blink-mode [enable|disable]
    set ekahau-tag {mac-address}
    set erc-server-ip {ipv4-address-any}
    set erc-server-port {integer}
    set aeroscout [enable|disable]
    set aeroscout-server-ip {ipv4-address-any}
    set aeroscout-server-port {integer}
    set aeroscout-mu [enable|disable]
    set aeroscout-ap-mac [bssid|board-mac]
    set aeroscout-mmu-report [enable|disable]
    set aeroscout-mu-factor {integer}
    set aeroscout-mu-timeout {integer}

```



```

    set fortipresence [foreign|both|...]
    set fortipresence-server-addr-type [ipv4|fqdn]
    set fortipresence-server {ipv4-address-any}
    set fortipresence-server-fqdn {string}
    set fortipresence-port {integer}
    set fortipresence-secret {password}
    set fortipresence-project {string}
    set fortipresence-frequency {integer}
    set fortipresence-rogue [enable|disable]
    set fortipresence-unassoc [enable|disable]
    set fortipresence-ble [enable|disable]
    set station-locate [enable|disable]
end
set led-schedules <name1>, <name2>, ...
set led-state [enable|disable]
set lldp [enable|disable]
set login-passwd {password}
set login-passwd-change [yes|default|...]
set max-clients {integer}
config platform
    Description: WTP, FortiAP, or AP platform.
    set type [AP-11N|220B|...]
    set mode [single-5G|dual-5G]
    set ddscan [enable|disable]
end
set poe-mode [auto|8023af|...]
config radio-1
    Description: Configuration options for radio 1.
    set mode [disabled|ap|...]
    set band [802.11a|802.11b|...]
    set band-5g-type [5g-full|5g-high|...]
    set drma [disable|enable]
    set drma-sensitivity [low|medium|...]
    set airtime-fairness [enable|disable]
    set protection-mode [rtscts|ctsonly|...]
    set powersave-optimize {option1}, {option2}, ...
    set transmit-optimize {option1}, {option2}, ...
    set amsdu [enable|disable]
    set coexistence [enable|disable]
    set zero-wait-dfs [enable|disable]
    set bss-color {integer}
    set bss-color-mode [auto|static]
    set short-guard-interval [enable|disable]
    set channel-bonding [160MHz|80MHz|...]
    set auto-power-level [enable|disable]
    set auto-power-high {integer}
    set auto-power-low {integer}
    set auto-power-target {string}
    set power-mode [dBm|percentage]
    set power-level {integer}
    set power-value {integer}
    set dtim {integer}
    set beacon-interval {integer}
    set rts-threshold {integer}
    set frag-threshold {integer}
    set ap-sniffer-bufsize {integer}

```

```

set ap-sniffer-chan {integer}
set ap-sniffer-addr {mac-address}
set ap-sniffer-mgmt-beacon [enable|disable]
set ap-sniffer-mgmt-probe [enable|disable]
set ap-sniffer-mgmt-other [enable|disable]
set ap-sniffer-ctl [enable|disable]
set ap-sniffer-data [enable|disable]
set sam-ssid {string}
set sam-bssid {mac-address}
set sam-security-type [open|wpa-personal|...]
set sam-captive-portal [enable|disable]
set sam-cwp-username {string}
set sam-cwp-password {password}
set sam-cwp-test-url {string}
set sam-cwp-match-string {string}
set sam-cwp-success-string {string}
set sam-cwp-failure-string {string}
set sam-username {string}
set sam-password {password}
set sam-test [ping|iperf]
set sam-server-type [ip|fqdn]
set sam-server-ip {ipv4-address}
set sam-server-fqdn {string}
set iperf-server-port {integer}
set iperf-protocol [udp|tcp]
set sam-report-intv {integer}
set channel-utilization [enable|disable]
set wids-profile {string}
set darrp [enable|disable]
set arrp-profile {string}
set max-clients {integer}
set max-distance {integer}
set vap-all [tunnel|bridge|...]
set vaps <name1>, <name2>, ...
set channel <chan1>, <chan2>, ...
set call-admission-control [enable|disable]
set call-capacity {integer}
set bandwidth-admission-control [enable|disable]
set bandwidth-capacity {integer}
end
config radio-2
  Description: Configuration options for radio 2.
  set mode [disabled|ap|...]
  set band [802.11a|802.11b|...]
  set band-5g-type [5g-full|5g-high|...]
  set drma [disable|enable]
  set drma-sensitivity [low|medium|...]
  set airtime-fairness [enable|disable]
  set protection-mode [rtscts|ctsonly|...]
  set powersave-optimize {option1}, {option2}, ...
  set transmit-optimize {option1}, {option2}, ...
  set amsdu [enable|disable]
  set coexistence [enable|disable]
  set zero-wait-dfs [enable|disable]
  set bss-color {integer}
  set bss-color-mode [auto|static]

```

```
set short-guard-interval [enable|disable]
set channel-bonding [160MHz|80MHz|...]
set auto-power-level [enable|disable]
set auto-power-high {integer}
set auto-power-low {integer}
set auto-power-target {string}
set power-mode [dBm|percentage]
set power-level {integer}
set power-value {integer}
set dtim {integer}
set beacon-interval {integer}
set rts-threshold {integer}
set frag-threshold {integer}
set ap-sniffer-bufsize {integer}
set ap-sniffer-chan {integer}
set ap-sniffer-addr {mac-address}
set ap-sniffer-mgmt-beacon [enable|disable]
set ap-sniffer-mgmt-probe [enable|disable]
set ap-sniffer-mgmt-other [enable|disable]
set ap-sniffer-ctl [enable|disable]
set ap-sniffer-data [enable|disable]
set sam-ssid {string}
set sam-bssid {mac-address}
set sam-security-type [open|wpa-personal|...]
set sam-captive-portal [enable|disable]
set sam-cwp-username {string}
set sam-cwp-password {password}
set sam-cwp-test-url {string}
set sam-cwp-match-string {string}
set sam-cwp-success-string {string}
set sam-cwp-failure-string {string}
set sam-username {string}
set sam-password {password}
set sam-test [ping|iperf]
set sam-server-type [ip|fqdn]
set sam-server-ip {ipv4-address}
set sam-server-fqdn {string}
set iperf-server-port {integer}
set iperf-protocol [udp|tcp]
set sam-report-intv {integer}
set channel-utilization [enable|disable]
set wids-profile {string}
set darrp [enable|disable]
set arrp-profile {string}
set max-clients {integer}
set max-distance {integer}
set vap-all [tunnel|bridge|...]
set vaps <name1>, <name2>, ...
set channel <chan1>, <chan2>, ...
set call-admission-control [enable|disable]
set call-capacity {integer}
set bandwidth-admission-control [enable|disable]
set bandwidth-capacity {integer}
end
config radio-3
    Description: Configuration options for radio 3.
```

---

```
set mode [disabled|ap|...]
set band [802.11a|802.11b|...]
set band-5g-type [5g-full|5g-high|...]
set drma [disable|enable]
set drma-sensitivity [low|medium|...]
set airtime-fairness [enable|disable]
set protection-mode [rtscts|ctsonly|...]
set powersave-optimize {option1}, {option2}, ...
set transmit-optimize {option1}, {option2}, ...
set amsdu [enable|disable]
set coexistence [enable|disable]
set zero-wait-dfs [enable|disable]
set bss-color {integer}
set bss-color-mode [auto|static]
set short-guard-interval [enable|disable]
set channel-bonding [160MHz|80MHz|...]
set auto-power-level [enable|disable]
set auto-power-high {integer}
set auto-power-low {integer}
set auto-power-target {string}
set power-mode [dBm|percentage]
set power-level {integer}
set power-value {integer}
set dtim {integer}
set beacon-interval {integer}
set rts-threshold {integer}
set frag-threshold {integer}
set ap-sniffer-bufsize {integer}
set ap-sniffer-chan {integer}
set ap-sniffer-addr {mac-address}
set ap-sniffer-mgmt-beacon [enable|disable]
set ap-sniffer-mgmt-probe [enable|disable]
set ap-sniffer-mgmt-other [enable|disable]
set ap-sniffer-ctl [enable|disable]
set ap-sniffer-data [enable|disable]
set sam-ssid {string}
set sam-bssid {mac-address}
set sam-security-type [open|wpa-personal|...]
set sam-captive-portal [enable|disable]
set sam-cwp-username {string}
set sam-cwp-password {password}
set sam-cwp-test-url {string}
set sam-cwp-match-string {string}
set sam-cwp-success-string {string}
set sam-cwp-failure-string {string}
set sam-username {string}
set sam-password {password}
set sam-test [ping|iperf]
set sam-server-type [ip|fqdn]
set sam-server-ip {ipv4-address}
set sam-server-fqdn {string}
set iperf-server-port {integer}
set iperf-protocol [udp|tcp]
set sam-report-intv {integer}
set channel-utilization [enable|disable]
set wids-profile {string}
```

```

set darrp [enable|disable]
set arrp-profile {string}
set max-clients {integer}
set max-distance {integer}
set vap-all [tunnel|bridge|...]
set vaps <name1>, <name2>, ...
set channel <chan1>, <chan2>, ...
set call-admission-control [enable|disable]
set call-capacity {integer}
set bandwidth-admission-control [enable|disable]
set bandwidth-capacity {integer}
end
config radio-4
  Description: Configuration options for radio 4.
  set mode [disabled|ap|...]
  set band [802.11a|802.11b|...]
  set band-5g-type [5g-full|5g-high|...]
  set drma [disable|enable]
  set drma-sensitivity [low|medium|...]
  set airtime-fairness [enable|disable]
  set protection-mode [rtscts|ctsonly|...]
  set powersave-optimize {option1}, {option2}, ...
  set transmit-optimize {option1}, {option2}, ...
  set amsdu [enable|disable]
  set coexistence [enable|disable]
  set zero-wait-dfs [enable|disable]
  set bss-color {integer}
  set bss-color-mode [auto|static]
  set short-guard-interval [enable|disable]
  set channel-bonding [160MHz|80MHz|...]
  set auto-power-level [enable|disable]
  set auto-power-high {integer}
  set auto-power-low {integer}
  set auto-power-target {string}
  set power-mode [dBm|percentage]
  set power-level {integer}
  set power-value {integer}
  set dtim {integer}
  set beacon-interval {integer}
  set rts-threshold {integer}
  set frag-threshold {integer}
  set ap-sniffer-bufsize {integer}
  set ap-sniffer-chan {integer}
  set ap-sniffer-addr {mac-address}
  set ap-sniffer-mgmt-beacon [enable|disable]
  set ap-sniffer-mgmt-probe [enable|disable]
  set ap-sniffer-mgmt-other [enable|disable]
  set ap-sniffer-ctl [enable|disable]
  set ap-sniffer-data [enable|disable]
  set sam-ssid {string}
  set sam-bssid {mac-address}
  set sam-security-type [open|wpa-personal|...]
  set sam-captive-portal [enable|disable]
  set sam-cwp-username {string}
  set sam-cwp-password {password}
  set sam-cwp-test-url {string}

```

```

        set sam-cwp-match-string {string}
        set sam-cwp-success-string {string}
        set sam-cwp-failure-string {string}
        set sam-username {string}
        set sam-password {password}
        set sam-test [ping|iperf]
        set sam-server-type [ip|fqdn]
        set sam-server-ip {ipv4-address}
        set sam-server-fqdn {string}
        set iperf-server-port {integer}
        set iperf-protocol [udp|tcp]
        set sam-report-intv {integer}
        set channel-utilization [enable|disable]
        set wids-profile {string}
        set darrp [enable|disable]
        set arrp-profile {string}
        set max-clients {integer}
        set max-distance {integer}
        set vap-all [tunnel|bridge|...]
        set vaps <name1>, <name2>, ...
        set channel <chan1>, <chan2>, ...
        set call-admission-control [enable|disable]
        set call-capacity {integer}
        set bandwidth-admission-control [enable|disable]
        set bandwidth-capacity {integer}
    end
    config split-tunneling-acl
        Description: Split tunneling ACL filter list.
        edit <id>
            set dest-ip {ipv4-classnet}
        next
    end
    set split-tunneling-acl-local-ap-subnet [enable|disable]
    set split-tunneling-acl-path [tunnel|local]
    set syslog-profile {string}
    set tun-mtu-downlink {integer}
    set tun-mtu-uplink {integer}
    set wan-port-auth [none|802.1x]
    set wan-port-auth-methods [all|EAP-FAST|...]
    set wan-port-auth-password {password}
    set wan-port-auth-username {string}
    set wan-port-mode [wan-lan|wan-only]
next
end

```

## config wireless-controller wtp-profile

Parameter	Description	Type	Size	Default
allowaccess	Control management access to the managed WTP, FortiAP, or AP. Separate entries with a space.	option	-	

Parameter	Description	Type	Size	Default																																														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>https</i></td><td>HTTPS access.</td></tr><tr><td><i>ssh</i></td><td>SSH access.</td></tr><tr><td><i>snmp</i></td><td>SNMP access.</td></tr></table>	Option	Description	<i>https</i>	HTTPS access.	<i>ssh</i>	SSH access.	<i>snmp</i>	SNMP access.																																									
	Option	Description																																																
	<i>https</i>	HTTPS access.																																																
	<i>ssh</i>	SSH access.																																																
<i>snmp</i>	SNMP access.																																																	
ap-country	Country in which this WTP, FortiAP, or AP will operate.	option	-	--																																														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>--</td><td>NO_COUNTRY_SET</td></tr><tr><td>AF</td><td>AFGHANISTAN</td></tr><tr><td>AL</td><td>ALBANIA</td></tr><tr><td>DZ</td><td>ALGERIA</td></tr><tr><td>AS</td><td>AMERICAN SAMOA</td></tr><tr><td>AO</td><td>ANGOLA</td></tr><tr><td>AR</td><td>ARGENTINA</td></tr><tr><td>AM</td><td>ARMENIA</td></tr><tr><td>AU</td><td>AUSTRALIA</td></tr><tr><td>AT</td><td>AUSTRIA</td></tr><tr><td>AZ</td><td>AZERBAIJAN</td></tr><tr><td>BS</td><td>BAHAMAS</td></tr><tr><td>BH</td><td>BAHRAIN</td></tr><tr><td>BD</td><td>BANGLADESH</td></tr><tr><td>BB</td><td>BARBADOS</td></tr><tr><td>BY</td><td>BELARUS</td></tr><tr><td>BE</td><td>BELGIUM</td></tr><tr><td>BZ</td><td>BELIZE</td></tr><tr><td>BJ</td><td>BENIN</td></tr><tr><td>BM</td><td>BERMUDA</td></tr><tr><td>BT</td><td>BHUTAN</td></tr><tr><td>BO</td><td>BOLIVIA</td></tr></table>	Option	Description	--	NO_COUNTRY_SET	AF	AFGHANISTAN	AL	ALBANIA	DZ	ALGERIA	AS	AMERICAN SAMOA	AO	ANGOLA	AR	ARGENTINA	AM	ARMENIA	AU	AUSTRALIA	AT	AUSTRIA	AZ	AZERBAIJAN	BS	BAHAMAS	BH	BAHRAIN	BD	BANGLADESH	BB	BARBADOS	BY	BELARUS	BE	BELGIUM	BZ	BELIZE	BJ	BENIN	BM	BERMUDA	BT	BHUTAN	BO	BOLIVIA			
	Option	Description																																																
	--	NO_COUNTRY_SET																																																
	AF	AFGHANISTAN																																																
	AL	ALBANIA																																																
	DZ	ALGERIA																																																
	AS	AMERICAN SAMOA																																																
	AO	ANGOLA																																																
	AR	ARGENTINA																																																
	AM	ARMENIA																																																
	AU	AUSTRALIA																																																
	AT	AUSTRIA																																																
	AZ	AZERBAIJAN																																																
	BS	BAHAMAS																																																
	BH	BAHRAIN																																																
	BD	BANGLADESH																																																
	BB	BARBADOS																																																
	BY	BELARUS																																																
	BE	BELGIUM																																																
	BZ	BELIZE																																																
	BJ	BENIN																																																
	BM	BERMUDA																																																
	BT	BHUTAN																																																
	BO	BOLIVIA																																																

Parameter	Description	Type	Size	Default
-----------	-------------	------	------	---------

Option	Description
<i>BA</i>	BOSNIA AND HERZEGOVINA
<i>BW</i>	BOTSWANA
<i>BR</i>	BRAZIL
<i>BN</i>	BRUNEI DARUSSALAM
<i>BG</i>	BULGARIA
<i>BF</i>	BURKINA-FASO
<i>KH</i>	CAMBODIA
<i>CM</i>	CAMEROON
<i>KY</i>	CAYMAN ISLANDS
<i>CF</i>	CENTRAL AFRICA REPUBLIC
<i>TD</i>	CHAD
<i>CL</i>	CHILE
<i>CN</i>	CHINA
<i>CX</i>	CHRISTMAS ISLAND
<i>CO</i>	COLOMBIA
<i>CG</i>	CONGO REPUBLIC
<i>CD</i>	DEMOCRATIC REPUBLIC OF CONGO
<i>CR</i>	COSTA RICA
<i>HR</i>	CROATIA
<i>CY</i>	CYPRUS
<i>CZ</i>	CZECH REPUBLIC
<i>DK</i>	DENMARK
<i>DM</i>	DOMINICA
<i>DO</i>	DOMINICAN REPUBLIC
<i>EC</i>	ECUADOR
<i>EG</i>	EGYPT
<i>SV</i>	EL SALVADOR
<i>ET</i>	ETHIOPIA
<i>EE</i>	ESTONIA



Parameter	Description	Type	Size	Default
	Option	Description		
	<i>GF</i>	FRENCH GUIANA		
	<i>PF</i>	FRENCH POLYNESIA		
	<i>FO</i>	FAEROE ISLANDS		
	<i>FJ</i>	FIJI		
	<i>FI</i>	FINLAND		
	<i>FR</i>	FRANCE		
	<i>GE</i>	GEORGIA		
	<i>DE</i>	GERMANY		
	<i>GH</i>	GHANA		
	<i>GI</i>	GIBRALTAR		
	<i>GR</i>	GREECE		
	<i>GL</i>	GREENLAND		
	<i>GD</i>	GRENADA		
	<i>GP</i>	GUADELOUPE		
	<i>GU</i>	GUAM		
	<i>GT</i>	GUATEMALA		
	<i>GY</i>	GUYANA		
	<i>HT</i>	HAITI		
	<i>HN</i>	HONDURAS		
	<i>HK</i>	HONG KONG		
	<i>HU</i>	HUNGARY		
	<i>IS</i>	ICELAND		
	<i>IN</i>	INDIA		
	<i>ID</i>	INDONESIA		
	<i>IQ</i>	IRAQ		
	<i>IE</i>	IRELAND		
	<i>IM</i>	ISLE OF MAN		
	<i>IL</i>	ISRAEL		
	<i>IT</i>	ITALY		

Parameter	Description	Type	Size	Default
-----------	-------------	------	------	---------

Option	Description
<i>CI</i>	COTE_D_IVOIRE
<i>JM</i>	JAMAICA
<i>JO</i>	JORDAN
<i>KZ</i>	KAZAKHSTAN
<i>KE</i>	KENYA
<i>KR</i>	KOREA REPUBLIC
<i>KW</i>	KUWAIT
<i>LA</i>	LAOS
<i>LV</i>	LATVIA
<i>LB</i>	LEBANON
<i>LS</i>	LESOTHO
<i>LY</i>	LIBYA
<i>LI</i>	LIECHTENSTEIN
<i>LT</i>	LITHUANIA
<i>LU</i>	LUXEMBOURG
<i>MO</i>	MACAU SAR
<i>MK</i>	MACEDONIA, FYRO
<i>MG</i>	MADAGASCAR
<i>MW</i>	MALAWI
<i>MY</i>	MALAYSIA
<i>MV</i>	MALDIVES
<i>ML</i>	MALI
<i>MT</i>	MALTA
<i>MH</i>	MARSHALL ISLANDS
<i>MQ</i>	MARTINIQUE
<i>MR</i>	MAURITANIA
<i>MU</i>	MAURITIUS
<i>YT</i>	MAYOTTE
<i>MX</i>	MEXICO

Parameter	Description	Type	Size	Default
-----------	-------------	------	------	---------

Option	Description
<i>FM</i>	MICRONESIA
<i>MD</i>	REPUBLIC OF MOLDOVA
<i>MC</i>	MONACO
<i>MN</i>	MONGOLIA
<i>MA</i>	MOROCCO
<i>MZ</i>	MOZAMBIQUE
<i>MM</i>	MYANMAR
<i>NA</i>	NAMIBIA
<i>NP</i>	NEPAL
<i>NL</i>	NETHERLANDS
<i>AN</i>	NETHERLANDS ANTILLES
<i>AW</i>	ARUBA
<i>NZ</i>	NEW ZEALAND
<i>NI</i>	NICARAGUA
<i>NE</i>	NIGER
<i>NO</i>	NORWAY
<i>MP</i>	NORTHERN MARIANA ISLANDS
<i>OM</i>	OMAN
<i>PK</i>	PAKISTAN
<i>PW</i>	PALAU
<i>PA</i>	PANAMA
<i>PG</i>	PAPUA NEW GUINEA
<i>PY</i>	PARAGUAY
<i>PE</i>	PERU
<i>PH</i>	PHILIPPINES
<i>PL</i>	POLAND
<i>PT</i>	PORTUGAL
<i>PR</i>	PUERTO RICO
<i>QA</i>	QATAR

Parameter	Description	Type	Size	Default
	Option	Description		
	<i>RE</i>	REUNION		
	<i>RO</i>	ROMANIA		
	<i>RU</i>	RUSSIA		
	<i>RW</i>	RWANDA		
	<i>BL</i>	SAINT BARTHELEMY		
	<i>KN</i>	SAINT KITTS AND NEVIS		
	<i>LC</i>	SAINT LUCIA		
	<i>MF</i>	SAINT MARTIN		
	<i>PM</i>	SAINT PIERRE AND MIQUELON		
	<i>VC</i>	SAINT VINCENT AND GRENADIENS		
	<i>SA</i>	SAUDI ARABIA		
	<i>SN</i>	SENEGAL		
	<i>RS</i>	REPUBLIC OF SERBIA		
	<i>ME</i>	MONTENEGRO		
	<i>SL</i>	SIERRA LEONE		
	<i>SG</i>	SINGAPORE		
	<i>SK</i>	SLOVAKIA		
	<i>SI</i>	SLOVENIA		
	<i>ZA</i>	SOUTH AFRICA		
	<i>ES</i>	SPAIN		
	<i>LK</i>	SRI LANKA		
	<i>SE</i>	SWEDEN		
	<i>SR</i>	SURINAME		
	<i>CH</i>	SWITZERLAND		
	<i>TW</i>	TAIWAN		
	<i>TZ</i>	TANZANIA		
	<i>TH</i>	THAILAND		
	<i>TG</i>	TOGO		
	<i>TT</i>	TRINIDAD AND TOBAGO		

Parameter	Description	Type	Size	Default																																														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>TN</i></td><td>TUNISIA</td></tr><tr><td><i>TR</i></td><td>TURKEY</td></tr><tr><td><i>TM</i></td><td>TURKMENISTAN</td></tr><tr><td><i>AE</i></td><td>UNITED ARAB EMIRATES</td></tr><tr><td><i>TC</i></td><td>TURKS AND CAICOS</td></tr><tr><td><i>UG</i></td><td>UGANDA</td></tr><tr><td><i>UA</i></td><td>UKRAINE</td></tr><tr><td><i>GB</i></td><td>UNITED KINGDOM</td></tr><tr><td><i>US</i></td><td>UNITED STATES2</td></tr><tr><td><i>PS</i></td><td>UNITED STATES (PUBLIC SAFETY)</td></tr><tr><td><i>UY</i></td><td>URUGUAY</td></tr><tr><td><i>UZ</i></td><td>UZBEKISTAN</td></tr><tr><td><i>VU</i></td><td>VANUATU</td></tr><tr><td><i>VE</i></td><td>VENEZUELA</td></tr><tr><td><i>VN</i></td><td>VIET NAM</td></tr><tr><td><i>VI</i></td><td>VIRGIN ISLANDS</td></tr><tr><td><i>WF</i></td><td>WALLIS AND FUTUNA</td></tr><tr><td><i>YE</i></td><td>YEMEN</td></tr><tr><td><i>ZM</i></td><td>ZAMBIA</td></tr><tr><td><i>ZW</i></td><td>ZIMBABWE</td></tr><tr><td><i>JP</i></td><td>JAPAN14</td></tr><tr><td><i>CA</i></td><td>CANADA2</td></tr></table>	Option	Description	<i>TN</i>	TUNISIA	<i>TR</i>	TURKEY	<i>TM</i>	TURKMENISTAN	<i>AE</i>	UNITED ARAB EMIRATES	<i>TC</i>	TURKS AND CAICOS	<i>UG</i>	UGANDA	<i>UA</i>	UKRAINE	<i>GB</i>	UNITED KINGDOM	<i>US</i>	UNITED STATES2	<i>PS</i>	UNITED STATES (PUBLIC SAFETY)	<i>UY</i>	URUGUAY	<i>UZ</i>	UZBEKISTAN	<i>VU</i>	VANUATU	<i>VE</i>	VENEZUELA	<i>VN</i>	VIET NAM	<i>VI</i>	VIRGIN ISLANDS	<i>WF</i>	WALLIS AND FUTUNA	<i>YE</i>	YEMEN	<i>ZM</i>	ZAMBIA	<i>ZW</i>	ZIMBABWE	<i>JP</i>	JAPAN14	<i>CA</i>	CANADA2			
	Option	Description																																																
	<i>TN</i>	TUNISIA																																																
	<i>TR</i>	TURKEY																																																
	<i>TM</i>	TURKMENISTAN																																																
	<i>AE</i>	UNITED ARAB EMIRATES																																																
	<i>TC</i>	TURKS AND CAICOS																																																
	<i>UG</i>	UGANDA																																																
	<i>UA</i>	UKRAINE																																																
	<i>GB</i>	UNITED KINGDOM																																																
	<i>US</i>	UNITED STATES2																																																
	<i>PS</i>	UNITED STATES (PUBLIC SAFETY)																																																
	<i>UY</i>	URUGUAY																																																
	<i>UZ</i>	UZBEKISTAN																																																
	<i>VU</i>	VANUATU																																																
	<i>VE</i>	VENEZUELA																																																
	<i>VN</i>	VIET NAM																																																
	<i>VI</i>	VIRGIN ISLANDS																																																
	<i>WF</i>	WALLIS AND FUTUNA																																																
	<i>YE</i>	YEMEN																																																
	<i>ZM</i>	ZAMBIA																																																
	<i>ZW</i>	ZIMBABWE																																																
	<i>JP</i>	JAPAN14																																																
<i>CA</i>	CANADA2																																																	
ap-handoff	Enable/disable AP handoff of clients to other APs.	option	-	disable																																														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable AP handoff.</td></tr><tr><td><i>disable</i></td><td>Disable AP handoff.</td></tr></table>	Option	Description	<i>enable</i>	Enable AP handoff.	<i>disable</i>	Disable AP handoff.																																											
	Option	Description																																																
	<i>enable</i>	Enable AP handoff.																																																
<i>disable</i>	Disable AP handoff.																																																	
apcfg-profile	AP local configuration profile name.	string	Maximum length: 35																																															
ble-profile	Bluetooth Low Energy profile name.	string	Maximum length: 35																																															

Parameter	Description	Type	Size	Default																				
comment	Comment.	var-string	Maximum length: 255																					
console-login	Enable/disable FortiAP console login access.	option	-	enable																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable FAP console login access.</td></tr><tr><td><i>disable</i></td><td>Disable FAP console login access.</td></tr></table>	Option	Description	<i>enable</i>	Enable FAP console login access.	<i>disable</i>	Disable FAP console login access.																	
Option	Description																							
<i>enable</i>	Enable FAP console login access.																							
<i>disable</i>	Disable FAP console login access.																							
control-message-offload	Enable/disable CAPWAP control message data channel offload.	option	-	ebp-frame aeroscout-tag ap-list sta-list sta-cap-list stats aeroscout-mu sta-health spectral-analysis																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ebp-frame</i></td><td>Ekahau blink protocol (EBP) frames.</td></tr><tr><td><i>aeroscout-tag</i></td><td>AeroScout tag.</td></tr><tr><td><i>ap-list</i></td><td>Rogue AP list.</td></tr><tr><td><i>sta-list</i></td><td>Rogue STA list.</td></tr><tr><td><i>sta-cap-list</i></td><td>STA capability list.</td></tr><tr><td><i>stats</i></td><td>WTP, radio, VAP, and STA statistics.</td></tr><tr><td><i>aeroscout-mu</i></td><td>AeroScout Mobile Unit (MU) report.</td></tr><tr><td><i>sta-health</i></td><td>STA health log.</td></tr><tr><td><i>spectral-analysis</i></td><td>Spectral analysis report.</td></tr></table>	Option	Description	<i>ebp-frame</i>	Ekahau blink protocol (EBP) frames.	<i>aeroscout-tag</i>	AeroScout tag.	<i>ap-list</i>	Rogue AP list.	<i>sta-list</i>	Rogue STA list.	<i>sta-cap-list</i>	STA capability list.	<i>stats</i>	WTP, radio, VAP, and STA statistics.	<i>aeroscout-mu</i>	AeroScout Mobile Unit (MU) report.	<i>sta-health</i>	STA health log.	<i>spectral-analysis</i>	Spectral analysis report.			
Option	Description																							
<i>ebp-frame</i>	Ekahau blink protocol (EBP) frames.																							
<i>aeroscout-tag</i>	AeroScout tag.																							
<i>ap-list</i>	Rogue AP list.																							
<i>sta-list</i>	Rogue STA list.																							
<i>sta-cap-list</i>	STA capability list.																							
<i>stats</i>	WTP, radio, VAP, and STA statistics.																							
<i>aeroscout-mu</i>	AeroScout Mobile Unit (MU) report.																							
<i>sta-health</i>	STA health log.																							
<i>spectral-analysis</i>	Spectral analysis report.																							
dtls-in-kernel	Enable/disable data channel DTLS in kernel.	option	-	disable																				
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable data channel DTLS in kernel.</td></tr><tr><td><i>disable</i></td><td>Disable data channel DTLS in kernel.</td></tr></table>	Option	Description	<i>enable</i>	Enable data channel DTLS in kernel.	<i>disable</i>	Disable data channel DTLS in kernel.																	
Option	Description																							
<i>enable</i>	Enable data channel DTLS in kernel.																							
<i>disable</i>	Disable data channel DTLS in kernel.																							
dtls-policy	WTP data channel DTLS policy.	option	-	clear-text																				

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>clear-text</i></td><td>Clear Text Data Channel.</td></tr><tr><td><i>dtls-enabled</i></td><td>DTLS Enabled Data Channel.</td></tr><tr><td><i>ipsec-vpn</i></td><td>IPsec VPN Data Channel.</td></tr></table>	Option	Description	<i>clear-text</i>	Clear Text Data Channel.	<i>dtls-enabled</i>	DTLS Enabled Data Channel.	<i>ipsec-vpn</i>	IPsec VPN Data Channel.			
	Option	Description										
	<i>clear-text</i>	Clear Text Data Channel.										
	<i>dtls-enabled</i>	DTLS Enabled Data Channel.										
<i>ipsec-vpn</i>	IPsec VPN Data Channel.											
energy-efficient-ethernet	Enable/disable use of energy efficient Ethernet on WTP.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable use of energy efficient Ethernet on WTP.</td></tr><tr><td><i>disable</i></td><td>Disable use of energy efficient Ethernet on WTP.</td></tr></table>	Option	Description	<i>enable</i>	Enable use of energy efficient Ethernet on WTP.	<i>disable</i>	Disable use of energy efficient Ethernet on WTP.					
	Option	Description										
	<i>enable</i>	Enable use of energy efficient Ethernet on WTP.										
<i>disable</i>	Disable use of energy efficient Ethernet on WTP.											
ext-info-enable	Enable/disable station/VAP/radio extension information.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable station/VAP/radio extension information.</td></tr><tr><td><i>disable</i></td><td>Disable station/VAP/radio extension information.</td></tr></table>	Option	Description	<i>enable</i>	Enable station/VAP/radio extension information.	<i>disable</i>	Disable station/VAP/radio extension information.					
	Option	Description										
	<i>enable</i>	Enable station/VAP/radio extension information.										
<i>disable</i>	Disable station/VAP/radio extension information.											
frequency-handoff	Enable/disable frequency handoff of clients to other channels.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable frequency handoff.</td></tr><tr><td><i>disable</i></td><td>Disable frequency handoff.</td></tr></table>	Option	Description	<i>enable</i>	Enable frequency handoff.	<i>disable</i>	Disable frequency handoff.					
	Option	Description										
	<i>enable</i>	Enable frequency handoff.										
<i>disable</i>	Disable frequency handoff.											
handoff-roaming	Enable/disable client load balancing during roaming to avoid roaming delay.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable handoff roaming.</td></tr><tr><td><i>disable</i></td><td>Disable handoff roaming.</td></tr></table>	Option	Description	<i>enable</i>	Enable handoff roaming.	<i>disable</i>	Disable handoff roaming.					
	Option	Description										
	<i>enable</i>	Enable handoff roaming.										
<i>disable</i>	Disable handoff roaming.											
handoff-rssi	Minimum received signal strength indicator.	integer	Minimum value: 20 Maximum value: 30	25								

Parameter	Description	Type	Size	Default								
handoff-sta-thresh	Threshold value for AP handoff.	integer	Minimum value: 0 Maximum value: 4294967295	0								
indoor-outdoor-deployment	Set to allow indoor/outdoor-only channels under regulatory rules.	option	-	platform-determined								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>platform-determined</td><td>Set AP deployment type based on its platform.</td></tr><tr><td>outdoor</td><td>Set AP deployment type to outdoor.</td></tr><tr><td>indoor</td><td>Set AP deployment type to indoor.</td></tr></table>				Option	Description	platform-determined	Set AP deployment type based on its platform.	outdoor	Set AP deployment type to outdoor.	indoor	Set AP deployment type to indoor.
Option	Description											
platform-determined	Set AP deployment type based on its platform.											
outdoor	Set AP deployment type to outdoor.											
indoor	Set AP deployment type to indoor.											
ip-fragment-preventing	Method.	option	-	tcp-mss-adjust								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>tcp-mss-adjust</td><td>TCP maximum segment size adjustment.</td></tr><tr><td>icmp-unreachable</td><td>Drop packet and send ICMP Destination Unreachable</td></tr></table>				Option	Description	tcp-mss-adjust	TCP maximum segment size adjustment.	icmp-unreachable	Drop packet and send ICMP Destination Unreachable		
Option	Description											
tcp-mss-adjust	TCP maximum segment size adjustment.											
icmp-unreachable	Drop packet and send ICMP Destination Unreachable											
led-schedules<name>	Recurring firewall schedules for illuminating LEDs on the FortiAP. If led-state is enabled, LEDs will be visible when at least one of the schedules is valid. Separate multiple schedule names with a space. Schedule name.	string	Maximum length: 35									
led-state	Enable/disable use of LEDs on WTP.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable use of LEDs on WTP.</td></tr><tr><td>disable</td><td>Disable use of LEDs on WTP.</td></tr></table>				Option	Description	enable	Enable use of LEDs on WTP.	disable	Disable use of LEDs on WTP.		
Option	Description											
enable	Enable use of LEDs on WTP.											
disable	Disable use of LEDs on WTP.											
lldp	Enable/disable Link Layer Discovery Protocol.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable LLDP.</td></tr><tr><td>disable</td><td>Disable LLDP.</td></tr></table>				Option	Description	enable	Enable LLDP.	disable	Disable LLDP.		
Option	Description											
enable	Enable LLDP.											
disable	Disable LLDP.											



Parameter	Description	Type	Size	Default																
login-passwd	Set the managed WTP, FortiAP, or AP's administrator password.	password	Not Specified																	
login-passwd-change	Change or reset the administrator password of a managed WTP, FortiAP or AP.	option	-	no																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>yes</i></td><td>Change the managed WTP, FortiAP or AP's administrator password. Use the login-password option to set the password.</td></tr><tr><td><i>default</i></td><td>Keep the managed WTP, FortiAP or AP's administrator password set to the factory default.</td></tr><tr><td><i>no</i></td><td>Do not change the managed WTP, FortiAP or AP's administrator password.</td></tr></table>	Option	Description	<i>yes</i>	Change the managed WTP, FortiAP or AP's administrator password. Use the login-password option to set the password.	<i>default</i>	Keep the managed WTP, FortiAP or AP's administrator password set to the factory default.	<i>no</i>	Do not change the managed WTP, FortiAP or AP's administrator password.											
Option	Description																			
<i>yes</i>	Change the managed WTP, FortiAP or AP's administrator password. Use the login-password option to set the password.																			
<i>default</i>	Keep the managed WTP, FortiAP or AP's administrator password set to the factory default.																			
<i>no</i>	Do not change the managed WTP, FortiAP or AP's administrator password.																			
max-clients	Maximum number of stations.	integer	Minimum value: 0 Maximum value: 4294967295	0																
name	WTP (or FortiAP or AP) profile name.	string	Maximum length: 35																	
poe-mode	Set the WTP, FortiAP, or AP's PoE mode.	option	-	auto																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto</i></td><td>Automatically detect the PoE mode.</td></tr><tr><td><i>8023af</i></td><td>Use 802.3af PoE mode.</td></tr><tr><td><i>8023at</i></td><td>Use 802.3at PoE mode.</td></tr><tr><td><i>power-adapter</i></td><td>Use the power adapter to control the PoE mode.</td></tr><tr><td><i>full</i></td><td>Use full power mode.</td></tr><tr><td><i>high</i></td><td>Use high power mode.</td></tr><tr><td><i>low</i></td><td>Use low power mode.</td></tr></table>	Option	Description	<i>auto</i>	Automatically detect the PoE mode.	<i>8023af</i>	Use 802.3af PoE mode.	<i>8023at</i>	Use 802.3at PoE mode.	<i>power-adapter</i>	Use the power adapter to control the PoE mode.	<i>full</i>	Use full power mode.	<i>high</i>	Use high power mode.	<i>low</i>	Use low power mode.			
Option	Description																			
<i>auto</i>	Automatically detect the PoE mode.																			
<i>8023af</i>	Use 802.3af PoE mode.																			
<i>8023at</i>	Use 802.3at PoE mode.																			
<i>power-adapter</i>	Use the power adapter to control the PoE mode.																			
<i>full</i>	Use full power mode.																			
<i>high</i>	Use high power mode.																			
<i>low</i>	Use low power mode.																			
split-tunneling-acl-local-ap-subnet	Enable/disable automatically adding local subnetwork of FortiAP to split-tunneling ACL.	option	-	disable																
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable automatically adding local subnetwork of FortiAP to split-tunneling ACL.</td></tr><tr><td><i>disable</i></td><td>Disable automatically adding local subnetwork of FortiAP to split-tunneling ACL.</td></tr></table>	Option	Description	<i>enable</i>	Enable automatically adding local subnetwork of FortiAP to split-tunneling ACL.	<i>disable</i>	Disable automatically adding local subnetwork of FortiAP to split-tunneling ACL.													
Option	Description																			
<i>enable</i>	Enable automatically adding local subnetwork of FortiAP to split-tunneling ACL.																			
<i>disable</i>	Disable automatically adding local subnetwork of FortiAP to split-tunneling ACL.																			

Parameter	Description	Type	Size	Default
split-tunneling-acl-path	Split tunneling ACL path is local/tunnel.	option	-	local
	<b>Option</b>	<b>Description</b>		
	<i>tunnel</i>	Split tunneling ACL list traffic will be tunnel.		
	<i>local</i>	Split tunneling ACL list traffic will be local NATed.		
syslog-profile	System log server configuration profile name.	string	Maximum length: 35	
tun-mtu-downlink	The MTU of downlink CAPWAP tunnel.	integer	Minimum value: 576 Maximum value: 1500	0
tun-mtu-uplink	The maximum transmission unit.	integer	Minimum value: 576 Maximum value: 1500	0
wan-port-auth	Set WAN port authentication mode.	option	-	none
	<b>Option</b>	<b>Description</b>		
	<i>none</i>	Disable WAN port authentication.		
	<i>802.1x</i>	Enable WAN port 802.1x authentication.		
wan-port-auth-methods	WAN port 802.1x supplicant EAP methods.	option	-	all
	<b>Option</b>	<b>Description</b>		
	<i>all</i>	Do not specify any EAP methods.		
	<i>EAP-FAST</i>	Enable EAP-FAST.		
	<i>EAP-TLS</i>	Enable EAP-TLS.		
	<i>EAP-PEAP</i>	Enable EAP-PEAP.		
wan-port-auth-password	Set WAN port 802.1x supplicant password.	password	Not Specified	
wan-port-auth-username	Set WAN port 802.1x supplicant user name.	string	Maximum length: 63	
wan-port-mode	Enable/disable using a WAN port as a LAN port.	option	-	wan-only

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>wan-lan</i>	Enable using a WAN port as a LAN port.		
	<i>wan-only</i>	Disable using a WAN port as a LAN port.		

### config deny-mac-list

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
mac	A WiFi device with this MAC address is denied access to this WTP, FortiAP or AP.	mac-address	Not Specified	00:00:00:00:00:00

### config esl-ses-dongle

Parameter	Description	Type	Size	Default
compliance-level	Compliance levels for the ESL solution integration.	option	-	compliance-level-2
	<b>Option</b>	<b>Description</b>		
	<i>compliance-level-2</i>	Compliance Level 2 - Full Cloud Support, IoT and Fast-Response.		
scd-enable	Enable/disable ESL SES-imagotag Serial Communication Daemon.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable ESL SES-imagotag SCD.		
	<i>disable</i>	Disable ESL SES-imagotag SCD.		
esl-channel	ESL SES-imagotag dongle channel.	option	-	127
	<b>Option</b>	<b>Description</b>		
	<i>-1</i>	No esl-channel is set.		
	<i>0</i>	ESL channel 0.		
	<i>1</i>	ESL channel 1.		

Parameter	Description	Type	Size	Default																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>2</td><td>ESL channel 2.</td></tr><tr><td>3</td><td>ESL channel 3.</td></tr><tr><td>4</td><td>ESL channel 4.</td></tr><tr><td>5</td><td>ESL channel 5.</td></tr><tr><td>6</td><td>ESL channel 6.</td></tr><tr><td>7</td><td>ESL channel 7.</td></tr><tr><td>8</td><td>ESL channel 8.</td></tr><tr><td>9</td><td>ESL channel 9.</td></tr><tr><td>10</td><td>ESL channel 10.</td></tr><tr><td>127</td><td>Managed channel enabled, indicates that the APC (server) is setting the esl-channel via the slot channel</td></tr></table>	Option	Description	2	ESL channel 2.	3	ESL channel 3.	4	ESL channel 4.	5	ESL channel 5.	6	ESL channel 6.	7	ESL channel 7.	8	ESL channel 8.	9	ESL channel 9.	10	ESL channel 10.	127	Managed channel enabled, indicates that the APC (server) is setting the esl-channel via the slot channel			
	Option	Description																								
	2	ESL channel 2.																								
	3	ESL channel 3.																								
	4	ESL channel 4.																								
	5	ESL channel 5.																								
	6	ESL channel 6.																								
	7	ESL channel 7.																								
	8	ESL channel 8.																								
	9	ESL channel 9.																								
	10	ESL channel 10.																								
127	Managed channel enabled, indicates that the APC (server) is setting the esl-channel via the slot channel																									
output-power	ESL SES-imagotag dongle output power.	option	-	a																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>a</td><td>About 15mW.</td></tr><tr><td>b</td><td>About 7mW.</td></tr><tr><td>c</td><td>About 5mW.</td></tr><tr><td>d</td><td>About 1mW.</td></tr><tr><td>e</td><td>About 13mW.</td></tr><tr><td>f</td><td>About 10mW.</td></tr><tr><td>g</td><td>About 3mW.</td></tr><tr><td>h</td><td>About 2mW.</td></tr></table>	Option	Description	a	About 15mW.	b	About 7mW.	c	About 5mW.	d	About 1mW.	e	About 13mW.	f	About 10mW.	g	About 3mW.	h	About 2mW.							
	Option	Description																								
	a	About 15mW.																								
	b	About 7mW.																								
	c	About 5mW.																								
	d	About 1mW.																								
	e	About 13mW.																								
	f	About 10mW.																								
	g	About 3mW.																								
h	About 2mW.																									
apc-addr-type	ESL SES-imagotag APC address type.	option	-	fqdn																						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>fqdn</td><td>Fully Qualified Domain Name address.</td></tr><tr><td>ip</td><td>IPv4 address.</td></tr></table>	Option	Description	fqdn	Fully Qualified Domain Name address.	ip	IPv4 address.																			
	Option	Description																								
	fqdn	Fully Qualified Domain Name address.																								
ip	IPv4 address.																									
apc-fqdn	FQDN of ESL SES-imagotag Access Point Controller (APC).	string	Maximum length: 63																							
apc-ip	IP address of ESL SES-imagotag Access Point Controller (APC).	ipv4-address	Not Specified	0.0.0.0																						

Parameter	Description	Type	Size	Default						
apc-port	Port of ESL SES-imagotag Access Point Controller (APC).	integer	Minimum value: 0 Maximum value: 65535	0						
coex-level	ESL SES-imagotag dongle coexistence level.	option	-	none						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>none</i></td><td>No support for coexistence of USB-Dongle with WiFi AP.</td></tr></table>				Option	Description	<i>none</i>	No support for coexistence of USB-Dongle with WiFi AP.		
Option	Description									
<i>none</i>	No support for coexistence of USB-Dongle with WiFi AP.									
tls-cert-verification	Enable/disable TLS certificate verification.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable TLS Certificate verification.</td></tr><tr><td><i>disable</i></td><td>Disable TLS Certificate verification.</td></tr></table>				Option	Description	<i>enable</i>	Enable TLS Certificate verification.	<i>disable</i>	Disable TLS Certificate verification.
Option	Description									
<i>enable</i>	Enable TLS Certificate verification.									
<i>disable</i>	Disable TLS Certificate verification.									
tls-fqdn-verification	Enable/disable TLS certificate verification.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable TLS FQDN verification.</td></tr><tr><td><i>disable</i></td><td>Disable TLS FQDN verification.</td></tr></table>				Option	Description	<i>enable</i>	Enable TLS FQDN verification.	<i>disable</i>	Disable TLS FQDN verification.
Option	Description									
<i>enable</i>	Enable TLS FQDN verification.									
<i>disable</i>	Disable TLS FQDN verification.									

## config lan

Parameter	Description	Type	Size	Default
port-mode	LAN port mode.	option	-	offline
	<b>Option</b>	<b>Description</b>		
	<i>offline</i>	Offline.		
	<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.		
	<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.		
	<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.		
port-ssid	Bridge LAN port to SSID.	string	Maximum length: 15	
port1-mode	LAN port 1 mode.	option	-	offline

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>offline</i>	Offline.		
	<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.		
	<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.		
	<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.		
port1-ssid	Bridge LAN port 1 to SSID.	string	Maximum length: 15	
port2-mode	LAN port 2 mode.	option	-	offline
	<b>Option</b>	<b>Description</b>		
	<i>offline</i>	Offline.		
	<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.		
	<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.		
	<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.		
port2-ssid	Bridge LAN port 2 to SSID.	string	Maximum length: 15	
port3-mode	LAN port 3 mode.	option	-	offline
	<b>Option</b>	<b>Description</b>		
	<i>offline</i>	Offline.		
	<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.		
	<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.		
	<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.		
port3-ssid	Bridge LAN port 3 to SSID.	string	Maximum length: 15	
port4-mode	LAN port 4 mode.	option	-	offline
	<b>Option</b>	<b>Description</b>		
	<i>offline</i>	Offline.		
	<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.		
	<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.		
	<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.		

Parameter	Description	Type	Size	Default
port4-ssid	Bridge LAN port 4 to SSID.	string	Maximum length: 15	
port5-mode	LAN port 5 mode.	option	-	offline
	<b>Option</b>	<b>Description</b>		
	<i>offline</i>	Offline.		
	<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.		
	<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.		
	<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.		
port5-ssid	Bridge LAN port 5 to SSID.	string	Maximum length: 15	
port6-mode	LAN port 6 mode.	option	-	offline
	<b>Option</b>	<b>Description</b>		
	<i>offline</i>	Offline.		
	<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.		
	<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.		
	<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.		
port6-ssid	Bridge LAN port 6 to SSID.	string	Maximum length: 15	
port7-mode	LAN port 7 mode.	option	-	offline
	<b>Option</b>	<b>Description</b>		
	<i>offline</i>	Offline.		
	<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.		
	<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.		
	<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.		
port7-ssid	Bridge LAN port 7 to SSID.	string	Maximum length: 15	
port8-mode	LAN port 8 mode.	option	-	offline
	<b>Option</b>	<b>Description</b>		
	<i>offline</i>	Offline.		
	<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.		

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.		
	<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.		
port8-ssid	Bridge LAN port 8 to SSID.	string	Maximum length: 15	
port-esl-mode	ESL port mode.	option	-	offline
	<b>Option</b>	<b>Description</b>		
	<i>offline</i>	Offline.		
	<i>nat-to-wan</i>	NAT WTP ESL port to WTP WAN port.		
	<i>bridge-to-wan</i>	Bridge WTP ESL port to WTP WAN port.		
	<i>bridge-to-ssid</i>	Bridge WTP ESL port to SSID.		
port-esl-ssid	Bridge ESL port to SSID.	string	Maximum length: 15	

## config lbs

Parameter	Description	Type	Size	Default						
ekahau-blink-mode	Enable/disable Ekahau blink mode.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Ekahau blink mode.</td></tr><tr><td><i>disable</i></td><td>Disable Ekahau blink mode.</td></tr></table>				Option	Description	<i>enable</i>	Enable Ekahau blink mode.	<i>disable</i>	Disable Ekahau blink mode.
	Option	Description								
	<i>enable</i>	Enable Ekahau blink mode.								
<i>disable</i>	Disable Ekahau blink mode.									
ekahau-tag	WiFi frame MAC address or WiFi Tag.	mac-address	Not Specified	01:18:8e:00:00:00						
erc-server-ip	IP address of Ekahau RTLS Controller (ERC).	ipv4-address-any	Not Specified	0.0.0.0						
erc-server-port	Ekahau RTLS Controller (ERC) UDP listening port.	integer	Minimum value: 1024 Maximum value: 65535	8569						
aeroscout	Enable/disable AeroScout Real Time Location Service.	option	-	disable						



Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable AeroScout support.		
	<i>disable</i>	Disable AeroScout support.		
aeroscout-server-ip	IP address of AeroScout server.	ipv4-address-any	Not Specified	0.0.0.0
aeroscout-server-port	AeroScout server UDP listening port.	integer	Minimum value: 1024 Maximum value: 65535	0
aeroscout-mu	Enable/disable AeroScout Mobile Unit.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable AeroScout MU mode support.		
	<i>disable</i>	Disable AeroScout MU mode support.		
aeroscout-ap-mac	Use BSSID or board MAC address as AP MAC address in AeroScout AP messages.	option	-	bssid
	<b>Option</b>	<b>Description</b>		
	<i>bssid</i>	Use BSSID as AP MAC address in AeroScout AP messages.		
	<i>board-mac</i>	Use board MAC address as AP MAC address in AeroScout AP messages.		
aeroscout-mmureport	Enable/disable compounded AeroScout tag and MU report.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable compounded AeroScout tag and MU report.		
	<i>disable</i>	Disable compounded AeroScout tag and MU report.		
aeroscout-mu-factor	AeroScout MU mode dilution factor.	integer	Minimum value: 0 Maximum value: 4294967295	20
aeroscout-mu-timeout	AeroScout MU mode timeout.	integer	Minimum value: 0 Maximum value: 65535	5

Parameter	Description	Type	Size	Default								
fortipresence	Enable/disable FortiPresence to monitor the location and activity of WiFi clients even if they don't connect to this WiFi network.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>foreign</i></td><td>FortiPresence monitors foreign channels only. Foreign channels mean all other available channels than the current operating channel of the WTP, AP, or FortiAP.</td></tr><tr><td><i>both</i></td><td>Enable FortiPresence on both foreign and home channels. Select this option to have FortiPresence monitor all WiFi channels.</td></tr><tr><td><i>disable</i></td><td>Disable FortiPresence.</td></tr></table>	Option	Description	<i>foreign</i>	FortiPresence monitors foreign channels only. Foreign channels mean all other available channels than the current operating channel of the WTP, AP, or FortiAP.	<i>both</i>	Enable FortiPresence on both foreign and home channels. Select this option to have FortiPresence monitor all WiFi channels.	<i>disable</i>	Disable FortiPresence.			
Option	Description											
<i>foreign</i>	FortiPresence monitors foreign channels only. Foreign channels mean all other available channels than the current operating channel of the WTP, AP, or FortiAP.											
<i>both</i>	Enable FortiPresence on both foreign and home channels. Select this option to have FortiPresence monitor all WiFi channels.											
<i>disable</i>	Disable FortiPresence.											
fortipresence-server-addr-type	FortiPresence server address type.	option	-	ipv4								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ipv4</i></td><td>IPv4 address.</td></tr><tr><td><i>fqdn</i></td><td>Fully Qualified Domain Name address.</td></tr></table>	Option	Description	<i>ipv4</i>	IPv4 address.	<i>fqdn</i>	Fully Qualified Domain Name address.					
Option	Description											
<i>ipv4</i>	IPv4 address.											
<i>fqdn</i>	Fully Qualified Domain Name address.											
fortipresence-server	IP address of FortiPresence server.	ipv4-address-any	Not Specified	0.0.0.0								
fortipresence-server-fqdn	FQDN of FortiPresence server.	string	Maximum length: 255									
fortipresence-port	UDP listening port of FortiPresence server.	integer	Minimum value: 300 Maximum value: 65535	3000								
fortipresence-secret	FortiPresence secret password (max. 16 characters).	password	Not Specified									
fortipresence-project	FortiPresence project name.	string	Maximum length: 16	fortipresence								
fortipresence-frequency	FortiPresence report transmit frequency.	integer	Minimum value: 5 Maximum value: 65535	30								
fortipresence-rogue	Enable/disable FortiPresence finding and reporting rogue APs.	option	-	disable								

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable FortiPresence finding and reporting rogue APs.		
	<i>disable</i>	Disable FortiPresence finding and reporting rogue APs.		
fortipresence-unassoc	Enable/disable FortiPresence finding and reporting unassociated stations.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable FortiPresence finding and reporting unassociated stations.		
	<i>disable</i>	Disable FortiPresence finding and reporting unassociated stations.		
fortipresence-ble	Enable/disable FortiPresence finding and reporting BLE devices.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable FortiPresence finding and reporting BLE devices.		
	<i>disable</i>	Disable FortiPresence finding and reporting BLE devices.		
station-locate	Enable/disable client station locating services for all clients, whether associated or not.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable station locating service.		
	<i>disable</i>	Disable station locating service.		

## config platform

Parameter	Description	Type	Size	Default
type	WTP, FortiAP or AP platform type. There are built-in WTP profiles for all supported FortiAP models. You can select a built-in profile and customize it or create a new profile.	option	-	221E
	<b>Option</b>	<b>Description</b>		
	<i>AP-11N</i>	Default 11n AP.		
	<i>220B</i>	FAP220B/221B.		
	<i>210B</i>	FAP210B.		
	<i>222B</i>	FAP222B.		

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	112B	FAP112B.		
	320B	FAP320B.		
	11C	FAP11C.		
	14C	FAP14C.		
	223B	FAP223B.		
	28C	FAP28C.		
	320C	FAP320C.		
	221C	FAP221C.		
	25D	FAP25D.		
	222C	FAP222C.		
	224D	FAP224D.		
	214B	FK214B.		
	21D	FAP21D.		
	24D	FAP24D.		
	112D	FAP112D.		
	223C	FAP223C.		
	321C	FAP321C.		
	C220C	FAPC220C.		
	C225C	FAPC225C.		
	C23JD	FAPC23JD.		
	C24JE	FAPC24JE.		
	S321C	FAPS321C.		
	S322C	FAPS322C.		
	S323C	FAPS323C.		
	S311C	FAPS311C.		
	S313C	FAPS313C.		
	S321CR	FAPS321CR.		
	S322CR	FAPS322CR.		
	S323CR	FAPS323CR.		

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>S421E</i>	FAPS421E.		
	<i>S422E</i>	FAPS422E.		
	<i>S423E</i>	FAPS423E.		
	<i>421E</i>	FAP421E.		
	<i>423E</i>	FAP423E.		
	<i>221E</i>	FAP221E.		
	<i>222E</i>	FAP222E.		
	<i>223E</i>	FAP223E.		
	<i>224E</i>	FAP224E.		
	<i>231E</i>	FAP231E.		
	<i>S221E</i>	FAPS221E.		
	<i>S223E</i>	FAPS223E.		
	<i>321E</i>	FAP321E.		
	<i>431F</i>	FAP431F.		
	<i>431FL</i>	FAP431FL.		
	<i>432F</i>	FAP432F.		
	<i>432FR</i>	FAP432FR.		
	<i>433F</i>	FAP433F.		
	<i>433FL</i>	FAP433FL.		
	<i>231F</i>	FAP231F.		
	<i>231FL</i>	FAP231FL.		
	<i>234F</i>	FAP234F.		
	<i>23JF</i>	FAP23JF.		
	<i>831F</i>	FAP831F.		
	<i>231G</i>	FAP231G.		
	<i>233G</i>	FAP233G.		
	<i>431G</i>	FAP431G.		
	<i>433G</i>	FAP433G.		
	<i>U421E</i>	FAPU421EV.		

Parameter	Description	Type	Size	Default																														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>U422EV</i></td><td>FAPU422EV.</td></tr><tr><td><i>U423E</i></td><td>FAPU423EV.</td></tr><tr><td><i>U221EV</i></td><td>FAPU221EV.</td></tr><tr><td><i>U223EV</i></td><td>FAPU223EV.</td></tr><tr><td><i>U24JEV</i></td><td>FAPU24JEV.</td></tr><tr><td><i>U321EV</i></td><td>FAPU321EV.</td></tr><tr><td><i>U323EV</i></td><td>FAPU323EV.</td></tr><tr><td><i>U431F</i></td><td>FAPU431F.</td></tr><tr><td><i>U433F</i></td><td>FAPU433F.</td></tr><tr><td><i>U231F</i></td><td>FAPU231F.</td></tr><tr><td><i>U234F</i></td><td>FAPU234F.</td></tr><tr><td><i>U432F</i></td><td>FAPU432F.</td></tr><tr><td><i>U231G</i></td><td>FAPU231G.</td></tr><tr><td><i>U441G</i></td><td>FAPU441G.</td></tr></table>	Option	Description	<i>U422EV</i>	FAPU422EV.	<i>U423E</i>	FAPU423EV.	<i>U221EV</i>	FAPU221EV.	<i>U223EV</i>	FAPU223EV.	<i>U24JEV</i>	FAPU24JEV.	<i>U321EV</i>	FAPU321EV.	<i>U323EV</i>	FAPU323EV.	<i>U431F</i>	FAPU431F.	<i>U433F</i>	FAPU433F.	<i>U231F</i>	FAPU231F.	<i>U234F</i>	FAPU234F.	<i>U432F</i>	FAPU432F.	<i>U231G</i>	FAPU231G.	<i>U441G</i>	FAPU441G.			
	Option	Description																																
	<i>U422EV</i>	FAPU422EV.																																
	<i>U423E</i>	FAPU423EV.																																
	<i>U221EV</i>	FAPU221EV.																																
	<i>U223EV</i>	FAPU223EV.																																
	<i>U24JEV</i>	FAPU24JEV.																																
	<i>U321EV</i>	FAPU321EV.																																
	<i>U323EV</i>	FAPU323EV.																																
	<i>U431F</i>	FAPU431F.																																
	<i>U433F</i>	FAPU433F.																																
	<i>U231F</i>	FAPU231F.																																
	<i>U234F</i>	FAPU234F.																																
	<i>U432F</i>	FAPU432F.																																
	<i>U231G</i>	FAPU231G.																																
<i>U441G</i>	FAPU441G.																																	
mode	Configure operation mode of 5G radios.	option	-	single-5G																														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>single-5G</i></td><td>Configure radios as one 5GHz band, one 2.4GHz band, and one dedicated monitor or sniffer.</td></tr><tr><td><i>dual-5G</i></td><td>Configure radios as one lower 5GHz band, one higher 5GHz band and one 2.4GHz band respectively.</td></tr></table>	Option	Description	<i>single-5G</i>	Configure radios as one 5GHz band, one 2.4GHz band, and one dedicated monitor or sniffer.	<i>dual-5G</i>	Configure radios as one lower 5GHz band, one higher 5GHz band and one 2.4GHz band respectively.																											
	Option	Description																																
	<i>single-5G</i>	Configure radios as one 5GHz band, one 2.4GHz band, and one dedicated monitor or sniffer.																																
<i>dual-5G</i>	Configure radios as one lower 5GHz band, one higher 5GHz band and one 2.4GHz band respectively.																																	
ddscan	Enable/disable use of one radio for dedicated full-band scanning to detect RF characterization and wireless threat management.	option	-	disable																														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable dedicated full-band scan mode.</td></tr><tr><td><i>disable</i></td><td>Disable dedicated full-band scan mode.</td></tr></table>	Option	Description	<i>enable</i>	Enable dedicated full-band scan mode.	<i>disable</i>	Disable dedicated full-band scan mode.																											
	Option	Description																																
	<i>enable</i>	Enable dedicated full-band scan mode.																																
<i>disable</i>	Disable dedicated full-band scan mode.																																	

## config radio-1

Parameter	Description	Type	Size	Default																																		
mode	Mode of radio 1. Radio 1 can be disabled, configured as an access point, a rogue AP monitor, a sniffer, or a station.	option	-	ap																																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disabled</i></td><td>Radio 1 is disabled.</td></tr><tr><td><i>ap</i></td><td>Radio 1 operates as an access point that allows WiFi clients to connect to your network.</td></tr><tr><td><i>monitor</i></td><td>Radio 1 operates as a dedicated monitor. As a monitor, the radio scans for other WiFi access points and adds them to the Rogue AP monitor list.</td></tr><tr><td><i>sniffer</i></td><td>Radio 1 operates as a sniffer capturing WiFi frames on air.</td></tr><tr><td><i>sam</i></td><td>Radio 1 operates as a station that can connect to a neighboring AP for connectivity and health check.</td></tr></table>	Option	Description	<i>disabled</i>	Radio 1 is disabled.	<i>ap</i>	Radio 1 operates as an access point that allows WiFi clients to connect to your network.	<i>monitor</i>	Radio 1 operates as a dedicated monitor. As a monitor, the radio scans for other WiFi access points and adds them to the Rogue AP monitor list.	<i>sniffer</i>	Radio 1 operates as a sniffer capturing WiFi frames on air.	<i>sam</i>	Radio 1 operates as a station that can connect to a neighboring AP for connectivity and health check.																									
Option	Description																																					
<i>disabled</i>	Radio 1 is disabled.																																					
<i>ap</i>	Radio 1 operates as an access point that allows WiFi clients to connect to your network.																																					
<i>monitor</i>	Radio 1 operates as a dedicated monitor. As a monitor, the radio scans for other WiFi access points and adds them to the Rogue AP monitor list.																																					
<i>sniffer</i>	Radio 1 operates as a sniffer capturing WiFi frames on air.																																					
<i>sam</i>	Radio 1 operates as a station that can connect to a neighboring AP for connectivity and health check.																																					
band	WiFi band that Radio 1 operates on.	option	-																																			
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>802.11a</i></td><td>802.11a.</td></tr><tr><td><i>802.11b</i></td><td>802.11b.</td></tr><tr><td><i>802.11g</i></td><td>802.11g/b.</td></tr><tr><td><i>802.11n</i></td><td>802.11n/g/b at 2.4GHz.</td></tr><tr><td><i>802.11n-5G</i></td><td>802.11n/a at 5GHz.</td></tr><tr><td><i>802.11ac</i></td><td>802.11ac/n/a.</td></tr><tr><td><i>802.11ax-5G</i></td><td>802.11ax/ac/n/a at 5GHz.</td></tr><tr><td><i>802.11ax</i></td><td>802.11ax/n/g/b at 2.4GHz.</td></tr><tr><td><i>802.11ac-2G</i></td><td>802.11ac at 2.4GHz.</td></tr><tr><td><i>802.11ax-6G</i></td><td>802.11ax at 6GHz.</td></tr><tr><td><i>802.11n,g-only</i></td><td>802.11n/g at 2.4GHz.</td></tr><tr><td><i>802.11g-only</i></td><td>802.11g.</td></tr><tr><td><i>802.11n-only</i></td><td>802.11n at 2.4GHz.</td></tr><tr><td><i>802.11n-5G-only</i></td><td>802.11n at 5GHz.</td></tr><tr><td><i>802.11ac,n-only</i></td><td>802.11ac/n.</td></tr><tr><td><i>802.11ac-only</i></td><td>802.11ac.</td></tr></table>	Option	Description	<i>802.11a</i>	802.11a.	<i>802.11b</i>	802.11b.	<i>802.11g</i>	802.11g/b.	<i>802.11n</i>	802.11n/g/b at 2.4GHz.	<i>802.11n-5G</i>	802.11n/a at 5GHz.	<i>802.11ac</i>	802.11ac/n/a.	<i>802.11ax-5G</i>	802.11ax/ac/n/a at 5GHz.	<i>802.11ax</i>	802.11ax/n/g/b at 2.4GHz.	<i>802.11ac-2G</i>	802.11ac at 2.4GHz.	<i>802.11ax-6G</i>	802.11ax at 6GHz.	<i>802.11n,g-only</i>	802.11n/g at 2.4GHz.	<i>802.11g-only</i>	802.11g.	<i>802.11n-only</i>	802.11n at 2.4GHz.	<i>802.11n-5G-only</i>	802.11n at 5GHz.	<i>802.11ac,n-only</i>	802.11ac/n.	<i>802.11ac-only</i>	802.11ac.			
Option	Description																																					
<i>802.11a</i>	802.11a.																																					
<i>802.11b</i>	802.11b.																																					
<i>802.11g</i>	802.11g/b.																																					
<i>802.11n</i>	802.11n/g/b at 2.4GHz.																																					
<i>802.11n-5G</i>	802.11n/a at 5GHz.																																					
<i>802.11ac</i>	802.11ac/n/a.																																					
<i>802.11ax-5G</i>	802.11ax/ac/n/a at 5GHz.																																					
<i>802.11ax</i>	802.11ax/n/g/b at 2.4GHz.																																					
<i>802.11ac-2G</i>	802.11ac at 2.4GHz.																																					
<i>802.11ax-6G</i>	802.11ax at 6GHz.																																					
<i>802.11n,g-only</i>	802.11n/g at 2.4GHz.																																					
<i>802.11g-only</i>	802.11g.																																					
<i>802.11n-only</i>	802.11n at 2.4GHz.																																					
<i>802.11n-5G-only</i>	802.11n at 5GHz.																																					
<i>802.11ac,n-only</i>	802.11ac/n.																																					
<i>802.11ac-only</i>	802.11ac.																																					

Parameter	Description	Type	Size	Default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>802.11ax,ac-only</i></td><td>802.11ax/ac at 5GHz.</td></tr><tr><td><i>802.11ax,ac,n-only</i></td><td>802.11ax/ac/n at 5GHz.</td></tr><tr><td><i>802.11ax-5G-only</i></td><td>802.11ax at 5GHz.</td></tr><tr><td><i>802.11ax,n-only</i></td><td>802.11ax/n at 2.4GHz.</td></tr><tr><td><i>802.11ax,n,g-only</i></td><td>802.11ax/n/g at 2.4GHz.</td></tr><tr><td><i>802.11ax-only</i></td><td>802.11ax at 2.4GHz.</td></tr></table>	Option	Description	<i>802.11ax,ac-only</i>	802.11ax/ac at 5GHz.	<i>802.11ax,ac,n-only</i>	802.11ax/ac/n at 5GHz.	<i>802.11ax-5G-only</i>	802.11ax at 5GHz.	<i>802.11ax,n-only</i>	802.11ax/n at 2.4GHz.	<i>802.11ax,n,g-only</i>	802.11ax/n/g at 2.4GHz.	<i>802.11ax-only</i>	802.11ax at 2.4GHz.			
	Option	Description																
	<i>802.11ax,ac-only</i>	802.11ax/ac at 5GHz.																
	<i>802.11ax,ac,n-only</i>	802.11ax/ac/n at 5GHz.																
	<i>802.11ax-5G-only</i>	802.11ax at 5GHz.																
	<i>802.11ax,n-only</i>	802.11ax/n at 2.4GHz.																
	<i>802.11ax,n,g-only</i>	802.11ax/n/g at 2.4GHz.																
<i>802.11ax-only</i>	802.11ax at 2.4GHz.																	
band-5g-type	WiFi 5G band type.	option	-	5g-full														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>5g-full</i></td><td>Full 5G band.</td></tr><tr><td><i>5g-high</i></td><td>High 5G band.</td></tr><tr><td><i>5g-low</i></td><td>Low 5G band.</td></tr></table>	Option	Description	<i>5g-full</i>	Full 5G band.	<i>5g-high</i>	High 5G band.	<i>5g-low</i>	Low 5G band.									
	Option	Description																
	<i>5g-full</i>	Full 5G band.																
	<i>5g-high</i>	High 5G band.																
<i>5g-low</i>	Low 5G band.																	
drma	Enable/disable dynamic radio mode assignment.	option	-	disable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable dynamic radio mode assignment (DRMA).</td></tr><tr><td><i>enable</i></td><td>Enable dynamic radio mode assignment (DRMA).</td></tr></table>	Option	Description	<i>disable</i>	Disable dynamic radio mode assignment (DRMA).	<i>enable</i>	Enable dynamic radio mode assignment (DRMA).											
	Option	Description																
	<i>disable</i>	Disable dynamic radio mode assignment (DRMA).																
<i>enable</i>	Enable dynamic radio mode assignment (DRMA).																	
drma-sensitivity	Network Coverage Factor.	option	-	low														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>low</i></td><td>Consider a radio as redundant when its NCF is 100%.</td></tr><tr><td><i>medium</i></td><td>Consider a radio as redundant when its NCF is 95%.</td></tr><tr><td><i>high</i></td><td>Consider a radio as redundant when its NCF is 90%.</td></tr></table>	Option	Description	<i>low</i>	Consider a radio as redundant when its NCF is 100%.	<i>medium</i>	Consider a radio as redundant when its NCF is 95%.	<i>high</i>	Consider a radio as redundant when its NCF is 90%.									
	Option	Description																
	<i>low</i>	Consider a radio as redundant when its NCF is 100%.																
	<i>medium</i>	Consider a radio as redundant when its NCF is 95%.																
<i>high</i>	Consider a radio as redundant when its NCF is 90%.																	
airtime-fairness	Enable/disable airtime fairness.	option	-	disable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable airtime fairness (ATF) support.</td></tr><tr><td><i>disable</i></td><td>Disable airtime fairness (ATF) support.</td></tr></table>	Option	Description	<i>enable</i>	Enable airtime fairness (ATF) support.	<i>disable</i>	Disable airtime fairness (ATF) support.											
	Option	Description																
	<i>enable</i>	Enable airtime fairness (ATF) support.																
<i>disable</i>	Disable airtime fairness (ATF) support.																	



Parameter	Description	Type	Size	Default
protection-mode	Enable/disable 802.11g protection modes to support backwards compatibility with older clients (rtscts, ctsonly, disable).	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>rtscts</i>	Enable 802.11g protection RTS/CTS mode.		
	<i>ctsonly</i>	Enable 802.11g protection CTS only mode.		
	<i>disable</i>	Disable 802.11g protection mode.		
powersave-optimize	Enable client power-saving features such as TIM, AC VO, and OBSS etc.	option	-	
	<b>Option</b>	<b>Description</b>		
	<i>tim</i>	TIM bit for client in power save mode.		
	<i>ac-vo</i>	Use AC VO priority to send out packets in the power save queue.		
	<i>no-obss-scan</i>	Do not put OBSS scan IE into beacon and probe response frames.		
	<i>no-11b-rate</i>	Do not send frame using 11b data rate.		
	<i>client-rate-follow</i>	Adapt transmitting PHY rate with receiving PHY rate from a client.		
transmit-optimize	Packet transmission optimization options including power saving, aggregation limiting, retry limiting, etc. All are enabled by default.	option	-	power-save aggr-limit retry-limit send-bar
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable packet transmission optimization.		
	<i>power-save</i>	Tag client as operating in power save mode if excessive transmit retries occur.		
	<i>aggr-limit</i>	Set aggregation limit to a lower value when data rate is low.		
	<i>retry-limit</i>	Set software retry limit to a lower value when data rate is low.		
	<i>send-bar</i>	Limit transmission of BAR frames.		
amsdu	Enable/disable 802.11n AMSDU support. AMSDU can improve performance if supported by your WiFi clients.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable AMSDU support.		
	<i>disable</i>	Disable AMSDU support.		

Parameter	Description	Type	Size	Default										
coexistence	Enable/disable allowing both HT20 and HT40 on the same radio.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable support for both HT20 and HT40 on the same radio.</td></tr><tr><td><i>disable</i></td><td>Disable support for both HT20 and HT40 on the same radio.</td></tr></table>	Option	Description	<i>enable</i>	Enable support for both HT20 and HT40 on the same radio.	<i>disable</i>	Disable support for both HT20 and HT40 on the same radio.							
Option	Description													
<i>enable</i>	Enable support for both HT20 and HT40 on the same radio.													
<i>disable</i>	Disable support for both HT20 and HT40 on the same radio.													
zero-wait-dfs	Enable/disable zero wait DFS on radio.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable zero wait DFS</td></tr><tr><td><i>disable</i></td><td>Disable zero wait DFS</td></tr></table>	Option	Description	<i>enable</i>	Enable zero wait DFS	<i>disable</i>	Disable zero wait DFS							
Option	Description													
<i>enable</i>	Enable zero wait DFS													
<i>disable</i>	Disable zero wait DFS													
bss-color	BSS color value for this 11ax radio.	integer	Minimum value: 0 Maximum value: 63	0										
bss-color-mode	BSS color mode for this 11ax radio.	option	-	auto										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto</i></td><td>Automatically select BSS color value on AP.</td></tr><tr><td><i>static</i></td><td>Set BSS color value on this radio based on 'bss-color' CLI.</td></tr></table>	Option	Description	<i>auto</i>	Automatically select BSS color value on AP.	<i>static</i>	Set BSS color value on this radio based on 'bss-color' CLI.							
Option	Description													
<i>auto</i>	Automatically select BSS color value on AP.													
<i>static</i>	Set BSS color value on this radio based on 'bss-color' CLI.													
short-guard-interval	Use either the short guard interval (Short GI) of 400 ns or the long guard interval (Long GI) of 800 ns.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Select the 400 ns short guard interval (Short GI).</td></tr><tr><td><i>disable</i></td><td>Select the 800 ns long guard interval (Long GI).</td></tr></table>	Option	Description	<i>enable</i>	Select the 400 ns short guard interval (Short GI).	<i>disable</i>	Select the 800 ns long guard interval (Long GI).							
Option	Description													
<i>enable</i>	Select the 400 ns short guard interval (Short GI).													
<i>disable</i>	Select the 800 ns long guard interval (Long GI).													
channel-bonding	Channel bandwidth: 160,80, 40, or 20MHz. Channels may use both 20 and 40 by enabling coexistence.	option	-	20MHz										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>160MHz</i></td><td>160 MHz channel width.</td></tr><tr><td><i>80MHz</i></td><td>80 MHz channel width.</td></tr><tr><td><i>40MHz</i></td><td>40 MHz channel width.</td></tr><tr><td><i>20MHz</i></td><td>20 MHz channel width.</td></tr></table>	Option	Description	<i>160MHz</i>	160 MHz channel width.	<i>80MHz</i>	80 MHz channel width.	<i>40MHz</i>	40 MHz channel width.	<i>20MHz</i>	20 MHz channel width.			
Option	Description													
<i>160MHz</i>	160 MHz channel width.													
<i>80MHz</i>	80 MHz channel width.													
<i>40MHz</i>	40 MHz channel width.													
<i>20MHz</i>	20 MHz channel width.													

Parameter	Description	Type	Size	Default						
auto-power-level	Enable/disable automatic power-level adjustment to prevent co-channel interference.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable automatic transmit power adjustment.</td></tr><tr><td><i>disable</i></td><td>Disable automatic transmit power adjustment.</td></tr></table>	Option	Description	<i>enable</i>	Enable automatic transmit power adjustment.	<i>disable</i>	Disable automatic transmit power adjustment.			
Option	Description									
<i>enable</i>	Enable automatic transmit power adjustment.									
<i>disable</i>	Disable automatic transmit power adjustment.									
auto-power-high	The upper bound of automatic transmit power adjustment in dBm (the actual range of transmit power depends on the AP platform type).	integer	Minimum value: 0 Maximum value: 4294967295	17						
auto-power-low	The lower bound of automatic transmit power adjustment in dBm (the actual range of transmit power depends on the AP platform type).	integer	Minimum value: 0 Maximum value: 4294967295	10						
auto-power-target	Target of automatic transmit power adjustment in dBm.	string	Maximum length: 7	-70						
power-mode	Set radio effective isotropic radiated power. This power takes into account both radio transmit power and antenna gain. Higher power level settings may be constrained by local regulatory requirements and AP capabilities.	option	-	percentage						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>dBm</i></td><td>Set radio EIRP power in dBm.</td></tr><tr><td><i>percentage</i></td><td>Set radio EIRP power by percentage.</td></tr></table>	Option	Description	<i>dBm</i>	Set radio EIRP power in dBm.	<i>percentage</i>	Set radio EIRP power by percentage.			
Option	Description									
<i>dBm</i>	Set radio EIRP power in dBm.									
<i>percentage</i>	Set radio EIRP power by percentage.									
power-level	Radio EIRP power level as a percentage of the maximum EIRP power.	integer	Minimum value: 0 Maximum value: 100	100						
power-value	Radio EIRP power in dBm.	integer	Minimum value: 1 Maximum value: 33	27						

Parameter	Description	Type	Size	Default						
dtim	Delivery Traffic Indication Map. Set higher to save battery life of WiFi client in power-save mode.	integer	Minimum value: 1 Maximum value: 255	1						
beacon-interval	Beacon interval. The time between beacon frames in milliseconds. Actual range of beacon interval depends on the AP platform type.	integer	Minimum value: 0 Maximum value: 65535	100						
rts-threshold	Maximum packet size for RTS transmissions, specifying the maximum size of a data packet before RTS/CTS.	integer	Minimum value: 256 Maximum value: 2346	2346						
frag-threshold	Maximum packet size that can be sent without fragmentation.	integer	Minimum value: 800 Maximum value: 2346	2346						
ap-sniffer-bufsize	Sniffer buffer size.	integer	Minimum value: 1 Maximum value: 32	16						
ap-sniffer-chan	Channel on which to operate the sniffer.	integer	Minimum value: 0 Maximum value: 4294967295	36						
ap-sniffer-addr	MAC address to monitor.	mac-address	Not Specified	00:00:00:00:00:00						
ap-sniffer-mgmt-beacon	Enable/disable sniffer on WiFi management Beacon frames.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable sniffer on WiFi management beacon frame.</td></tr><tr><td>disable</td><td>Disable sniffer on WiFi management beacon frame.</td></tr></table>				Option	Description	enable	Enable sniffer on WiFi management beacon frame.	disable	Disable sniffer on WiFi management beacon frame.
Option	Description									
enable	Enable sniffer on WiFi management beacon frame.									
disable	Disable sniffer on WiFi management beacon frame.									
ap-sniffer-mgmt-probe	Enable/disable sniffer on WiFi management probe frames.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable sniffer on WiFi management probe frame.</td></tr><tr><td>disable</td><td>Enable sniffer on WiFi management probe frame.</td></tr></table>				Option	Description	enable	Enable sniffer on WiFi management probe frame.	disable	Enable sniffer on WiFi management probe frame.
Option	Description									
enable	Enable sniffer on WiFi management probe frame.									
disable	Enable sniffer on WiFi management probe frame.									

Parameter	Description	Type	Size	Default								
ap-sniffer-mgmt-other	Enable/disable sniffer on WiFi management other frames .	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable sniffer on WiFi management other frame.</td></tr><tr><td><i>disable</i></td><td>Disable sniffer on WiFi management other frame.</td></tr></table>	Option	Description	<i>enable</i>	Enable sniffer on WiFi management other frame.	<i>disable</i>	Disable sniffer on WiFi management other frame.					
Option	Description											
<i>enable</i>	Enable sniffer on WiFi management other frame.											
<i>disable</i>	Disable sniffer on WiFi management other frame.											
ap-sniffer-ctl	Enable/disable sniffer on WiFi control frame.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable sniffer on WiFi control frame.</td></tr><tr><td><i>disable</i></td><td>Disable sniffer on WiFi control frame.</td></tr></table>	Option	Description	<i>enable</i>	Enable sniffer on WiFi control frame.	<i>disable</i>	Disable sniffer on WiFi control frame.					
Option	Description											
<i>enable</i>	Enable sniffer on WiFi control frame.											
<i>disable</i>	Disable sniffer on WiFi control frame.											
ap-sniffer-data	Enable/disable sniffer on WiFi data frame.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable sniffer on WiFi data frame</td></tr><tr><td><i>disable</i></td><td>Disable sniffer on WiFi data frame</td></tr></table>	Option	Description	<i>enable</i>	Enable sniffer on WiFi data frame	<i>disable</i>	Disable sniffer on WiFi data frame					
Option	Description											
<i>enable</i>	Enable sniffer on WiFi data frame											
<i>disable</i>	Disable sniffer on WiFi data frame											
sam-ssid	SSID for WiFi network.	string	Maximum length: 32									
sam-bssid	BSSID for WiFi network.	mac-address	Not Specified	00:00:00:00:00:00								
sam-security-type	Select WiFi network security type.	option	-	wpa-personal								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>open</i></td><td>Open.</td></tr><tr><td><i>wpa-personal</i></td><td>WPA/WPA2 personal.</td></tr><tr><td><i>wpa-enterprise</i></td><td>WPA/WPA2 enterprise.</td></tr></table>	Option	Description	<i>open</i>	Open.	<i>wpa-personal</i>	WPA/WPA2 personal.	<i>wpa-enterprise</i>	WPA/WPA2 enterprise.			
Option	Description											
<i>open</i>	Open.											
<i>wpa-personal</i>	WPA/WPA2 personal.											
<i>wpa-enterprise</i>	WPA/WPA2 enterprise.											
sam-captive-portal	Enable/disable Captive Portal Authentication.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Captive Portal Authentication.</td></tr><tr><td><i>disable</i></td><td>Disable Captive Portal Authentication.</td></tr></table>	Option	Description	<i>enable</i>	Enable Captive Portal Authentication.	<i>disable</i>	Disable Captive Portal Authentication.					
Option	Description											
<i>enable</i>	Enable Captive Portal Authentication.											
<i>disable</i>	Disable Captive Portal Authentication.											

Parameter	Description	Type	Size	Default						
sam-cwp-username	Username for captive portal authentication.	string	Maximum length: 35							
sam-cwp-password	Password for captive portal authentication.	password	Not Specified							
sam-cwp-test-url	Website the client is trying to access.	string	Maximum length: 255							
sam-cwp-match-string	Identification string from the captive portal login form.	string	Maximum length: 64							
sam-cwp-success-string	Success identification on the page after a successful login.	string	Maximum length: 64							
sam-cwp-failure-string	Failure identification on the page after an incorrect login.	string	Maximum length: 64							
sam-username	Username for WiFi network connection.	string	Maximum length: 35							
sam-password	Passphrase for WiFi network connection.	password	Not Specified							
sam-test	Select SAM test type.	option	-	ping						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ping</i></td><td>PING test.</td></tr><tr><td><i>iperf</i></td><td>IPERF test.</td></tr></table>				Option	Description	<i>ping</i>	PING test.	<i>iperf</i>	IPERF test.
Option	Description									
<i>ping</i>	PING test.									
<i>iperf</i>	IPERF test.									
sam-server-type	Select SAM server type.	option	-	ip						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ip</i></td><td>IPv4 address.</td></tr><tr><td><i>fqdn</i></td><td>Fully Qualified Domain Name address.</td></tr></table>				Option	Description	<i>ip</i>	IPv4 address.	<i>fqdn</i>	Fully Qualified Domain Name address.
Option	Description									
<i>ip</i>	IPv4 address.									
<i>fqdn</i>	Fully Qualified Domain Name address.									
sam-server-ip	SAM test server IP address.	ipv4-address	Not Specified	0.0.0.0						
sam-server-fqdn	SAM test server domain name.	string	Maximum length: 255							
iperf-server-port	Iperf service port number.	integer	Minimum value: 0 Maximum value: 65535	5001						
iperf-protocol	Iperf test protocol.	option	-	udp						

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>udp</i></td><td>UDP.</td></tr><tr><td><i>tcp</i></td><td>TCP.</td></tr></table>	Option	Description	<i>udp</i>	UDP.	<i>tcp</i>	TCP.			
	Option	Description								
	<i>udp</i>	UDP.								
<i>tcp</i>	TCP.									
sam-report-intv	SAM report interval (sec), 0 for a one-time report.	integer	Minimum value: 60 Maximum value: 864000	0						
channel-utilization	Enable/disable measuring channel utilization.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable measuring channel utilization.</td></tr><tr><td><i>disable</i></td><td>Disable measuring channel utilization.</td></tr></table>	Option	Description	<i>enable</i>	Enable measuring channel utilization.	<i>disable</i>	Disable measuring channel utilization.			
	Option	Description								
	<i>enable</i>	Enable measuring channel utilization.								
<i>disable</i>	Disable measuring channel utilization.									
wids-profile	Wireless Intrusion Detection System (WIDS) profile name to assign to the radio.	string	Maximum length: 35							
darrp	Enable/disable Distributed Automatic Radio Resource Provisioning.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable distributed automatic radio resource provisioning.</td></tr><tr><td><i>disable</i></td><td>Disable distributed automatic radio resource provisioning.</td></tr></table>	Option	Description	<i>enable</i>	Enable distributed automatic radio resource provisioning.	<i>disable</i>	Disable distributed automatic radio resource provisioning.			
	Option	Description								
	<i>enable</i>	Enable distributed automatic radio resource provisioning.								
<i>disable</i>	Disable distributed automatic radio resource provisioning.									
arrp-profile	Distributed Automatic Radio Resource Provisioning (DARRP) profile name to assign to the radio.	string	Maximum length: 35							
max-clients	Maximum number of stations (STAs) or WiFi clients supported by the radio. Range depends on the hardware.	integer	Minimum value: 0 Maximum value: 4294967295	0						
max-distance	Maximum expected distance between the AP and clients.	integer	Minimum value: 0 Maximum value: 54000	0						
vap-all	Configure method for assigning SSIDs to this FortiAP.	option	-	tunnel						

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>tunnel</i></td><td>Automatically select tunnel SSIDs.</td></tr><tr><td><i>bridge</i></td><td>Automatically select local-bridging SSIDs.</td></tr><tr><td><i>manual</i></td><td>Manually select SSIDs.</td></tr></table>	Option	Description	<i>tunnel</i>	Automatically select tunnel SSIDs.	<i>bridge</i>	Automatically select local-bridging SSIDs.	<i>manual</i>	Manually select SSIDs.			
	Option	Description										
	<i>tunnel</i>	Automatically select tunnel SSIDs.										
	<i>bridge</i>	Automatically select local-bridging SSIDs.										
<i>manual</i>	Manually select SSIDs.											
vaps <name>	Manually selected list of Virtual Access Points (VAPs). Virtual Access Point (VAP) name.	string	Maximum length: 35									
channel <chan>	Selected list of wireless radio channels. Channel number.	string	Maximum length: 3									
call-admission-control	Enable/disable WiFi multimedia (WMM) call admission control to optimize WiFi bandwidth use for VoIP calls. New VoIP calls are only accepted if there is enough bandwidth available to support them.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable WMM call admission control.</td></tr><tr><td><i>disable</i></td><td>Disable WMM call admission control.</td></tr></table>	Option	Description	<i>enable</i>	Enable WMM call admission control.	<i>disable</i>	Disable WMM call admission control.					
	Option	Description										
	<i>enable</i>	Enable WMM call admission control.										
<i>disable</i>	Disable WMM call admission control.											
call-capacity	Maximum number of Voice over WLAN.	integer	Minimum value: 0 Maximum value: 60	10								
bandwidth-admission-control	Enable/disable WiFi multimedia (WMM) bandwidth admission control to optimize WiFi bandwidth use. A request to join the wireless network is only allowed if the access point has enough bandwidth to support it.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable WMM bandwidth admission control.</td></tr><tr><td><i>disable</i></td><td>Disable WMM bandwidth admission control.</td></tr></table>	Option	Description	<i>enable</i>	Enable WMM bandwidth admission control.	<i>disable</i>	Disable WMM bandwidth admission control.					
	Option	Description										
	<i>enable</i>	Enable WMM bandwidth admission control.										
<i>disable</i>	Disable WMM bandwidth admission control.											
bandwidth-capacity	Maximum bandwidth capacity allowed.	integer	Minimum value: 1 Maximum value: 600000	2000								



## config radio-2

Parameter	Description	Type	Size	Default																																		
mode	Mode of radio 2. Radio 2 can be disabled, configured as an access point, a rogue AP monitor, a sniffer, or a station.	option	-	ap																																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disabled</i></td><td>Radio 2 is disabled.</td></tr><tr><td><i>ap</i></td><td>Radio 2 operates as an access point that allows WiFi clients to connect to your network.</td></tr><tr><td><i>monitor</i></td><td>Radio 2 operates as a dedicated monitor. As a monitor, the radio scans for other WiFi access points and adds them to the Rogue AP monitor list.</td></tr><tr><td><i>sniffer</i></td><td>Radio 2 operates as a sniffer capturing WiFi frames on air.</td></tr><tr><td><i>sam</i></td><td>Radio 2 operates as a station that can connect to a neighboring AP for connectivity and health check.</td></tr></table>	Option	Description	<i>disabled</i>	Radio 2 is disabled.	<i>ap</i>	Radio 2 operates as an access point that allows WiFi clients to connect to your network.	<i>monitor</i>	Radio 2 operates as a dedicated monitor. As a monitor, the radio scans for other WiFi access points and adds them to the Rogue AP monitor list.	<i>sniffer</i>	Radio 2 operates as a sniffer capturing WiFi frames on air.	<i>sam</i>	Radio 2 operates as a station that can connect to a neighboring AP for connectivity and health check.																									
Option	Description																																					
<i>disabled</i>	Radio 2 is disabled.																																					
<i>ap</i>	Radio 2 operates as an access point that allows WiFi clients to connect to your network.																																					
<i>monitor</i>	Radio 2 operates as a dedicated monitor. As a monitor, the radio scans for other WiFi access points and adds them to the Rogue AP monitor list.																																					
<i>sniffer</i>	Radio 2 operates as a sniffer capturing WiFi frames on air.																																					
<i>sam</i>	Radio 2 operates as a station that can connect to a neighboring AP for connectivity and health check.																																					
band	WiFi band that Radio 2 operates on.	option	-																																			
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>802.11a</i></td><td>802.11a.</td></tr><tr><td><i>802.11b</i></td><td>802.11b.</td></tr><tr><td><i>802.11g</i></td><td>802.11g/b.</td></tr><tr><td><i>802.11n</i></td><td>802.11n/g/b at 2.4GHz.</td></tr><tr><td><i>802.11n-5G</i></td><td>802.11n/a at 5GHz.</td></tr><tr><td><i>802.11ac</i></td><td>802.11ac/n/a.</td></tr><tr><td><i>802.11ax-5G</i></td><td>802.11ax/ac/n/a at 5GHz.</td></tr><tr><td><i>802.11ax</i></td><td>802.11ax/n/g/b at 2.4GHz.</td></tr><tr><td><i>802.11ac-2G</i></td><td>802.11ac at 2.4GHz.</td></tr><tr><td><i>802.11ax-6G</i></td><td>802.11ax at 6GHz.</td></tr><tr><td><i>802.11n,g-only</i></td><td>802.11n/g at 2.4GHz.</td></tr><tr><td><i>802.11g-only</i></td><td>802.11g.</td></tr><tr><td><i>802.11n-only</i></td><td>802.11n at 2.4GHz.</td></tr><tr><td><i>802.11n-5G-only</i></td><td>802.11n at 5GHz.</td></tr><tr><td><i>802.11ac,n-only</i></td><td>802.11ac/n.</td></tr><tr><td><i>802.11ac-only</i></td><td>802.11ac.</td></tr></table>	Option	Description	<i>802.11a</i>	802.11a.	<i>802.11b</i>	802.11b.	<i>802.11g</i>	802.11g/b.	<i>802.11n</i>	802.11n/g/b at 2.4GHz.	<i>802.11n-5G</i>	802.11n/a at 5GHz.	<i>802.11ac</i>	802.11ac/n/a.	<i>802.11ax-5G</i>	802.11ax/ac/n/a at 5GHz.	<i>802.11ax</i>	802.11ax/n/g/b at 2.4GHz.	<i>802.11ac-2G</i>	802.11ac at 2.4GHz.	<i>802.11ax-6G</i>	802.11ax at 6GHz.	<i>802.11n,g-only</i>	802.11n/g at 2.4GHz.	<i>802.11g-only</i>	802.11g.	<i>802.11n-only</i>	802.11n at 2.4GHz.	<i>802.11n-5G-only</i>	802.11n at 5GHz.	<i>802.11ac,n-only</i>	802.11ac/n.	<i>802.11ac-only</i>	802.11ac.			
Option	Description																																					
<i>802.11a</i>	802.11a.																																					
<i>802.11b</i>	802.11b.																																					
<i>802.11g</i>	802.11g/b.																																					
<i>802.11n</i>	802.11n/g/b at 2.4GHz.																																					
<i>802.11n-5G</i>	802.11n/a at 5GHz.																																					
<i>802.11ac</i>	802.11ac/n/a.																																					
<i>802.11ax-5G</i>	802.11ax/ac/n/a at 5GHz.																																					
<i>802.11ax</i>	802.11ax/n/g/b at 2.4GHz.																																					
<i>802.11ac-2G</i>	802.11ac at 2.4GHz.																																					
<i>802.11ax-6G</i>	802.11ax at 6GHz.																																					
<i>802.11n,g-only</i>	802.11n/g at 2.4GHz.																																					
<i>802.11g-only</i>	802.11g.																																					
<i>802.11n-only</i>	802.11n at 2.4GHz.																																					
<i>802.11n-5G-only</i>	802.11n at 5GHz.																																					
<i>802.11ac,n-only</i>	802.11ac/n.																																					
<i>802.11ac-only</i>	802.11ac.																																					

Parameter	Description	Type	Size	Default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>802.11ax,ac-only</td><td>802.11ax/ac at 5GHz.</td></tr><tr><td>802.11ax,ac,n-only</td><td>802.11ax/ac/n at 5GHz.</td></tr><tr><td>802.11ax-5G-only</td><td>802.11ax at 5GHz.</td></tr><tr><td>802.11ax,n-only</td><td>802.11ax/n at 2.4GHz.</td></tr><tr><td>802.11ax,n,g-only</td><td>802.11ax/n/g at 2.4GHz.</td></tr><tr><td>802.11ax-only</td><td>802.11ax at 2.4GHz.</td></tr></table>	Option	Description	802.11ax,ac-only	802.11ax/ac at 5GHz.	802.11ax,ac,n-only	802.11ax/ac/n at 5GHz.	802.11ax-5G-only	802.11ax at 5GHz.	802.11ax,n-only	802.11ax/n at 2.4GHz.	802.11ax,n,g-only	802.11ax/n/g at 2.4GHz.	802.11ax-only	802.11ax at 2.4GHz.			
	Option	Description																
	802.11ax,ac-only	802.11ax/ac at 5GHz.																
	802.11ax,ac,n-only	802.11ax/ac/n at 5GHz.																
	802.11ax-5G-only	802.11ax at 5GHz.																
	802.11ax,n-only	802.11ax/n at 2.4GHz.																
	802.11ax,n,g-only	802.11ax/n/g at 2.4GHz.																
802.11ax-only	802.11ax at 2.4GHz.																	
band-5g-type	WiFi 5G band type.	option	-	5g-full														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>5g-full</td><td>Full 5G band.</td></tr><tr><td>5g-high</td><td>High 5G band.</td></tr><tr><td>5g-low</td><td>Low 5G band.</td></tr></table>	Option	Description	5g-full	Full 5G band.	5g-high	High 5G band.	5g-low	Low 5G band.									
	Option	Description																
	5g-full	Full 5G band.																
	5g-high	High 5G band.																
5g-low	Low 5G band.																	
drma	Enable/disable dynamic radio mode assignment.	option	-	disable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable dynamic radio mode assignment (DRMA).</td></tr><tr><td>enable</td><td>Enable dynamic radio mode assignment (DRMA).</td></tr></table>	Option	Description	disable	Disable dynamic radio mode assignment (DRMA).	enable	Enable dynamic radio mode assignment (DRMA).											
	Option	Description																
	disable	Disable dynamic radio mode assignment (DRMA).																
enable	Enable dynamic radio mode assignment (DRMA).																	
drma-sensitivity	Network Coverage Factor.	option	-	low														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>low</td><td>Consider a radio as redundant when its NCF is 100%.</td></tr><tr><td>medium</td><td>Consider a radio as redundant when its NCF is 95%.</td></tr><tr><td>high</td><td>Consider a radio as redundant when its NCF is 90%.</td></tr></table>	Option	Description	low	Consider a radio as redundant when its NCF is 100%.	medium	Consider a radio as redundant when its NCF is 95%.	high	Consider a radio as redundant when its NCF is 90%.									
	Option	Description																
	low	Consider a radio as redundant when its NCF is 100%.																
	medium	Consider a radio as redundant when its NCF is 95%.																
high	Consider a radio as redundant when its NCF is 90%.																	
airtime-fairness	Enable/disable airtime fairness.	option	-	disable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable airtime fairness (ATF) support.</td></tr><tr><td>disable</td><td>Disable airtime fairness (ATF) support.</td></tr></table>	Option	Description	enable	Enable airtime fairness (ATF) support.	disable	Disable airtime fairness (ATF) support.											
	Option	Description																
	enable	Enable airtime fairness (ATF) support.																
disable	Disable airtime fairness (ATF) support.																	

Parameter	Description	Type	Size	Default
protection-mode	Enable/disable 802.11g protection modes to support backwards compatibility with older clients (rtscts, ctsonly, disable).	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>rtscts</i>	Enable 802.11g protection RTS/CTS mode.		
	<i>ctsonly</i>	Enable 802.11g protection CTS only mode.		
	<i>disable</i>	Disable 802.11g protection mode.		
powersave-optimize	Enable client power-saving features such as TIM, AC VO, and OBSS etc.	option	-	
	<b>Option</b>	<b>Description</b>		
	<i>tim</i>	TIM bit for client in power save mode.		
	<i>ac-vo</i>	Use AC VO priority to send out packets in the power save queue.		
	<i>no-obss-scan</i>	Do not put OBSS scan IE into beacon and probe response frames.		
	<i>no-11b-rate</i>	Do not send frame using 11b data rate.		
	<i>client-rate-follow</i>	Adapt transmitting PHY rate with receiving PHY rate from a client.		
transmit-optimize	Packet transmission optimization options including power saving, aggregation limiting, retry limiting, etc. All are enabled by default.	option	-	power-save aggr-limit retry-limit send-bar
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable packet transmission optimization.		
	<i>power-save</i>	Tag client as operating in power save mode if excessive transmit retries occur.		
	<i>aggr-limit</i>	Set aggregation limit to a lower value when data rate is low.		
	<i>retry-limit</i>	Set software retry limit to a lower value when data rate is low.		
	<i>send-bar</i>	Limit transmission of BAR frames.		
amsdu	Enable/disable 802.11n AMSDU support. AMSDU can improve performance if supported by your WiFi clients.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable AMSDU support.		
	<i>disable</i>	Disable AMSDU support.		

Parameter	Description	Type	Size	Default										
coexistence	Enable/disable allowing both HT20 and HT40 on the same radio.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable support for both HT20 and HT40 on the same radio.</td></tr><tr><td><i>disable</i></td><td>Disable support for both HT20 and HT40 on the same radio.</td></tr></table>	Option	Description	<i>enable</i>	Enable support for both HT20 and HT40 on the same radio.	<i>disable</i>	Disable support for both HT20 and HT40 on the same radio.							
Option	Description													
<i>enable</i>	Enable support for both HT20 and HT40 on the same radio.													
<i>disable</i>	Disable support for both HT20 and HT40 on the same radio.													
zero-wait-dfs	Enable/disable zero wait DFS on radio.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable zero wait DFS</td></tr><tr><td><i>disable</i></td><td>Disable zero wait DFS</td></tr></table>	Option	Description	<i>enable</i>	Enable zero wait DFS	<i>disable</i>	Disable zero wait DFS							
Option	Description													
<i>enable</i>	Enable zero wait DFS													
<i>disable</i>	Disable zero wait DFS													
bss-color	BSS color value for this 11ax radio.	integer	Minimum value: 0 Maximum value: 63	0										
bss-color-mode	BSS color mode for this 11ax radio.	option	-	auto										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto</i></td><td>Automatically select BSS color value on AP.</td></tr><tr><td><i>static</i></td><td>Set BSS color value on this radio based on 'bss-color' CLI.</td></tr></table>	Option	Description	<i>auto</i>	Automatically select BSS color value on AP.	<i>static</i>	Set BSS color value on this radio based on 'bss-color' CLI.							
Option	Description													
<i>auto</i>	Automatically select BSS color value on AP.													
<i>static</i>	Set BSS color value on this radio based on 'bss-color' CLI.													
short-guard-interval	Use either the short guard interval (Short GI) of 400 ns or the long guard interval (Long GI) of 800 ns.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Select the 400 ns short guard interval (Short GI).</td></tr><tr><td><i>disable</i></td><td>Select the 800 ns long guard interval (Long GI).</td></tr></table>	Option	Description	<i>enable</i>	Select the 400 ns short guard interval (Short GI).	<i>disable</i>	Select the 800 ns long guard interval (Long GI).							
Option	Description													
<i>enable</i>	Select the 400 ns short guard interval (Short GI).													
<i>disable</i>	Select the 800 ns long guard interval (Long GI).													
channel-bonding	Channel bandwidth: 160,80, 40, or 20MHz. Channels may use both 20 and 40 by enabling coexistence.	option	-	20MHz										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>160MHz</i></td><td>160 MHz channel width.</td></tr><tr><td><i>80MHz</i></td><td>80 MHz channel width.</td></tr><tr><td><i>40MHz</i></td><td>40 MHz channel width.</td></tr><tr><td><i>20MHz</i></td><td>20 MHz channel width.</td></tr></table>	Option	Description	<i>160MHz</i>	160 MHz channel width.	<i>80MHz</i>	80 MHz channel width.	<i>40MHz</i>	40 MHz channel width.	<i>20MHz</i>	20 MHz channel width.			
Option	Description													
<i>160MHz</i>	160 MHz channel width.													
<i>80MHz</i>	80 MHz channel width.													
<i>40MHz</i>	40 MHz channel width.													
<i>20MHz</i>	20 MHz channel width.													

Parameter	Description	Type	Size	Default						
auto-power-level	Enable/disable automatic power-level adjustment to prevent co-channel interference.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable automatic transmit power adjustment.</td></tr><tr><td><i>disable</i></td><td>Disable automatic transmit power adjustment.</td></tr></table>	Option	Description	<i>enable</i>	Enable automatic transmit power adjustment.	<i>disable</i>	Disable automatic transmit power adjustment.			
Option	Description									
<i>enable</i>	Enable automatic transmit power adjustment.									
<i>disable</i>	Disable automatic transmit power adjustment.									
auto-power-high	The upper bound of automatic transmit power adjustment in dBm (the actual range of transmit power depends on the AP platform type).	integer	Minimum value: 0 Maximum value: 4294967295	17						
auto-power-low	The lower bound of automatic transmit power adjustment in dBm (the actual range of transmit power depends on the AP platform type).	integer	Minimum value: 0 Maximum value: 4294967295	10						
auto-power-target	Target of automatic transmit power adjustment in dBm.	string	Maximum length: 7	-70						
power-mode	Set radio effective isotropic radiated power. This power takes into account both radio transmit power and antenna gain. Higher power level settings may be constrained by local regulatory requirements and AP capabilities.	option	-	percentage						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>dBm</i></td><td>Set radio EIRP power in dBm.</td></tr><tr><td><i>percentage</i></td><td>Set radio EIRP power by percentage.</td></tr></table>	Option	Description	<i>dBm</i>	Set radio EIRP power in dBm.	<i>percentage</i>	Set radio EIRP power by percentage.			
Option	Description									
<i>dBm</i>	Set radio EIRP power in dBm.									
<i>percentage</i>	Set radio EIRP power by percentage.									
power-level	Radio EIRP power level as a percentage of the maximum EIRP power.	integer	Minimum value: 0 Maximum value: 100	100						
power-value	Radio EIRP power in dBm.	integer	Minimum value: 1 Maximum value: 33	27						

Parameter	Description	Type	Size	Default						
dtim	Delivery Traffic Indication Map. Set higher to save battery life of WiFi client in power-save mode.	integer	Minimum value: 1 Maximum value: 255	1						
beacon-interval	Beacon interval. The time between beacon frames in milliseconds. Actual range of beacon interval depends on the AP platform type.	integer	Minimum value: 0 Maximum value: 65535	100						
rts-threshold	Maximum packet size for RTS transmissions, specifying the maximum size of a data packet before RTS/CTS.	integer	Minimum value: 256 Maximum value: 2346	2346						
frag-threshold	Maximum packet size that can be sent without fragmentation.	integer	Minimum value: 800 Maximum value: 2346	2346						
ap-sniffer-bufsize	Sniffer buffer size.	integer	Minimum value: 1 Maximum value: 32	16						
ap-sniffer-chan	Channel on which to operate the sniffer.	integer	Minimum value: 0 Maximum value: 4294967295	6						
ap-sniffer-addr	MAC address to monitor.	mac-address	Not Specified	00:00:00:00:00:00						
ap-sniffer-mgmt-beacon	Enable/disable sniffer on WiFi management Beacon frames.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable sniffer on WiFi management beacon frame.</td></tr><tr><td>disable</td><td>Disable sniffer on WiFi management beacon frame.</td></tr></table>				Option	Description	enable	Enable sniffer on WiFi management beacon frame.	disable	Disable sniffer on WiFi management beacon frame.
Option	Description									
enable	Enable sniffer on WiFi management beacon frame.									
disable	Disable sniffer on WiFi management beacon frame.									
ap-sniffer-mgmt-probe	Enable/disable sniffer on WiFi management probe frames.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable sniffer on WiFi management probe frame.</td></tr><tr><td>disable</td><td>Enable sniffer on WiFi management probe frame.</td></tr></table>				Option	Description	enable	Enable sniffer on WiFi management probe frame.	disable	Enable sniffer on WiFi management probe frame.
Option	Description									
enable	Enable sniffer on WiFi management probe frame.									
disable	Enable sniffer on WiFi management probe frame.									

Parameter	Description	Type	Size	Default								
ap-sniffer-mgmt-other	Enable/disable sniffer on WiFi management other frames .	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable sniffer on WiFi management other frame.</td></tr><tr><td><i>disable</i></td><td>Disable sniffer on WiFi management other frame.</td></tr></table>	Option	Description	<i>enable</i>	Enable sniffer on WiFi management other frame.	<i>disable</i>	Disable sniffer on WiFi management other frame.					
Option	Description											
<i>enable</i>	Enable sniffer on WiFi management other frame.											
<i>disable</i>	Disable sniffer on WiFi management other frame.											
ap-sniffer-ctl	Enable/disable sniffer on WiFi control frame.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable sniffer on WiFi control frame.</td></tr><tr><td><i>disable</i></td><td>Disable sniffer on WiFi control frame.</td></tr></table>	Option	Description	<i>enable</i>	Enable sniffer on WiFi control frame.	<i>disable</i>	Disable sniffer on WiFi control frame.					
Option	Description											
<i>enable</i>	Enable sniffer on WiFi control frame.											
<i>disable</i>	Disable sniffer on WiFi control frame.											
ap-sniffer-data	Enable/disable sniffer on WiFi data frame.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable sniffer on WiFi data frame</td></tr><tr><td><i>disable</i></td><td>Disable sniffer on WiFi data frame</td></tr></table>	Option	Description	<i>enable</i>	Enable sniffer on WiFi data frame	<i>disable</i>	Disable sniffer on WiFi data frame					
Option	Description											
<i>enable</i>	Enable sniffer on WiFi data frame											
<i>disable</i>	Disable sniffer on WiFi data frame											
sam-ssid	SSID for WiFi network.	string	Maximum length: 32									
sam-bssid	BSSID for WiFi network.	mac-address	Not Specified	00:00:00:00:00:00								
sam-security-type	Select WiFi network security type.	option	-	wpa-personal								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>open</i></td><td>Open.</td></tr><tr><td><i>wpa-personal</i></td><td>WPA/WPA2 personal.</td></tr><tr><td><i>wpa-enterprise</i></td><td>WPA/WPA2 enterprise.</td></tr></table>	Option	Description	<i>open</i>	Open.	<i>wpa-personal</i>	WPA/WPA2 personal.	<i>wpa-enterprise</i>	WPA/WPA2 enterprise.			
Option	Description											
<i>open</i>	Open.											
<i>wpa-personal</i>	WPA/WPA2 personal.											
<i>wpa-enterprise</i>	WPA/WPA2 enterprise.											
sam-captive-portal	Enable/disable Captive Portal Authentication.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Captive Portal Authentication.</td></tr><tr><td><i>disable</i></td><td>Disable Captive Portal Authentication.</td></tr></table>	Option	Description	<i>enable</i>	Enable Captive Portal Authentication.	<i>disable</i>	Disable Captive Portal Authentication.					
Option	Description											
<i>enable</i>	Enable Captive Portal Authentication.											
<i>disable</i>	Disable Captive Portal Authentication.											

Parameter	Description	Type	Size	Default						
sam-cwp-username	Username for captive portal authentication.	string	Maximum length: 35							
sam-cwp-password	Password for captive portal authentication.	password	Not Specified							
sam-cwp-test-url	Website the client is trying to access.	string	Maximum length: 255							
sam-cwp-match-string	Identification string from the captive portal login form.	string	Maximum length: 64							
sam-cwp-success-string	Success identification on the page after a successful login.	string	Maximum length: 64							
sam-cwp-failure-string	Failure identification on the page after an incorrect login.	string	Maximum length: 64							
sam-username	Username for WiFi network connection.	string	Maximum length: 35							
sam-password	Passphrase for WiFi network connection.	password	Not Specified							
sam-test	Select SAM test type.	option	-	ping						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ping</i></td><td>PING test.</td></tr><tr><td><i>iperf</i></td><td>IPERF test.</td></tr></table>				Option	Description	<i>ping</i>	PING test.	<i>iperf</i>	IPERF test.
Option	Description									
<i>ping</i>	PING test.									
<i>iperf</i>	IPERF test.									
sam-server-type	Select SAM server type.	option	-	ip						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ip</i></td><td>IPv4 address.</td></tr><tr><td><i>fqdn</i></td><td>Fully Qualified Domain Name address.</td></tr></table>				Option	Description	<i>ip</i>	IPv4 address.	<i>fqdn</i>	Fully Qualified Domain Name address.
Option	Description									
<i>ip</i>	IPv4 address.									
<i>fqdn</i>	Fully Qualified Domain Name address.									
sam-server-ip	SAM test server IP address.	ipv4-address	Not Specified	0.0.0.0						
sam-server-fqdn	SAM test server domain name.	string	Maximum length: 255							
iperf-server-port	Iperf service port number.	integer	Minimum value: 0 Maximum value: 65535	5001						
iperf-protocol	Iperf test protocol.	option	-	udp						



Parameter	Description	Type	Size	Default							
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>udp</i></td><td>UDP.</td></tr><tr><td><i>tcp</i></td><td>TCP.</td></tr></table>		Option	Description	<i>udp</i>	UDP.	<i>tcp</i>	TCP.			
	Option	Description									
	<i>udp</i>	UDP.									
<i>tcp</i>	TCP.										
sam-report-intv	SAM report interval (sec), 0 for a one-time report.	integer	Minimum value: 60 Maximum value: 864000	0							
channel-utilization	Enable/disable measuring channel utilization.	option	-	enable							
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable measuring channel utilization.</td></tr><tr><td><i>disable</i></td><td>Disable measuring channel utilization.</td></tr></table>		Option	Description	<i>enable</i>	Enable measuring channel utilization.	<i>disable</i>	Disable measuring channel utilization.			
	Option	Description									
	<i>enable</i>	Enable measuring channel utilization.									
<i>disable</i>	Disable measuring channel utilization.										
wids-profile	Wireless Intrusion Detection System (WIDS) profile name to assign to the radio.	string	Maximum length: 35								
darrp	Enable/disable Distributed Automatic Radio Resource Provisioning.	option	-	disable							
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable distributed automatic radio resource provisioning.</td></tr><tr><td><i>disable</i></td><td>Disable distributed automatic radio resource provisioning.</td></tr></table>		Option	Description	<i>enable</i>	Enable distributed automatic radio resource provisioning.	<i>disable</i>	Disable distributed automatic radio resource provisioning.			
	Option	Description									
	<i>enable</i>	Enable distributed automatic radio resource provisioning.									
<i>disable</i>	Disable distributed automatic radio resource provisioning.										
arrp-profile	Distributed Automatic Radio Resource Provisioning (DARRP) profile name to assign to the radio.	string	Maximum length: 35								
max-clients	Maximum number of stations (STAs) or WiFi clients supported by the radio. Range depends on the hardware.	integer	Minimum value: 0 Maximum value: 4294967295	0							
max-distance	Maximum expected distance between the AP and clients.	integer	Minimum value: 0 Maximum value: 54000	0							
vap-all	Configure method for assigning SSIDs to this FortiAP.	option	-	tunnel							

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>tunnel</i></td><td>Automatically select tunnel SSIDs.</td></tr><tr><td><i>bridge</i></td><td>Automatically select local-bridging SSIDs.</td></tr><tr><td><i>manual</i></td><td>Manually select SSIDs.</td></tr></table>	Option	Description	<i>tunnel</i>	Automatically select tunnel SSIDs.	<i>bridge</i>	Automatically select local-bridging SSIDs.	<i>manual</i>	Manually select SSIDs.			
	Option	Description										
	<i>tunnel</i>	Automatically select tunnel SSIDs.										
	<i>bridge</i>	Automatically select local-bridging SSIDs.										
<i>manual</i>	Manually select SSIDs.											
vaps <name>	Manually selected list of Virtual Access Points (VAPs). Virtual Access Point (VAP) name.	string	Maximum length: 35									
channel <chan>	Selected list of wireless radio channels. Channel number.	string	Maximum length: 3									
call-admission-control	Enable/disable WiFi multimedia (WMM) call admission control to optimize WiFi bandwidth use for VoIP calls. New VoIP calls are only accepted if there is enough bandwidth available to support them.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable WMM call admission control.</td></tr><tr><td><i>disable</i></td><td>Disable WMM call admission control.</td></tr></table>	Option	Description	<i>enable</i>	Enable WMM call admission control.	<i>disable</i>	Disable WMM call admission control.					
	Option	Description										
	<i>enable</i>	Enable WMM call admission control.										
<i>disable</i>	Disable WMM call admission control.											
call-capacity	Maximum number of Voice over WLAN.	integer	Minimum value: 0 Maximum value: 60	10								
bandwidth-admission-control	Enable/disable WiFi multimedia (WMM) bandwidth admission control to optimize WiFi bandwidth use. A request to join the wireless network is only allowed if the access point has enough bandwidth to support it.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable WMM bandwidth admission control.</td></tr><tr><td><i>disable</i></td><td>Disable WMM bandwidth admission control.</td></tr></table>	Option	Description	<i>enable</i>	Enable WMM bandwidth admission control.	<i>disable</i>	Disable WMM bandwidth admission control.					
	Option	Description										
	<i>enable</i>	Enable WMM bandwidth admission control.										
<i>disable</i>	Disable WMM bandwidth admission control.											
bandwidth-capacity	Maximum bandwidth capacity allowed.	integer	Minimum value: 1 Maximum value: 600000	2000								

## config radio-3

Parameter	Description	Type	Size	Default																																		
mode	Mode of radio 3. Radio 3 can be disabled, configured as an access point, a rogue AP monitor, a sniffer, or a station.	option	-	ap																																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disabled</i></td><td>Radio 3 is disabled.</td></tr><tr><td><i>ap</i></td><td>Radio 3 operates as an access point that allows WiFi clients to connect to your network.</td></tr><tr><td><i>monitor</i></td><td>Radio 3 operates as a dedicated monitor. As a monitor, the radio scans for other WiFi access points and adds them to the Rogue AP monitor list.</td></tr><tr><td><i>sniffer</i></td><td>Radio 3 operates as a sniffer capturing WiFi frames on air.</td></tr><tr><td><i>sam</i></td><td>Radio 3 operates as a station that can connect to a neighboring AP for connectivity and health check.</td></tr></table>	Option	Description	<i>disabled</i>	Radio 3 is disabled.	<i>ap</i>	Radio 3 operates as an access point that allows WiFi clients to connect to your network.	<i>monitor</i>	Radio 3 operates as a dedicated monitor. As a monitor, the radio scans for other WiFi access points and adds them to the Rogue AP monitor list.	<i>sniffer</i>	Radio 3 operates as a sniffer capturing WiFi frames on air.	<i>sam</i>	Radio 3 operates as a station that can connect to a neighboring AP for connectivity and health check.																									
Option	Description																																					
<i>disabled</i>	Radio 3 is disabled.																																					
<i>ap</i>	Radio 3 operates as an access point that allows WiFi clients to connect to your network.																																					
<i>monitor</i>	Radio 3 operates as a dedicated monitor. As a monitor, the radio scans for other WiFi access points and adds them to the Rogue AP monitor list.																																					
<i>sniffer</i>	Radio 3 operates as a sniffer capturing WiFi frames on air.																																					
<i>sam</i>	Radio 3 operates as a station that can connect to a neighboring AP for connectivity and health check.																																					
band	WiFi band that Radio 3 operates on.	option	-																																			
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>802.11a</i></td><td>802.11a.</td></tr><tr><td><i>802.11b</i></td><td>802.11b.</td></tr><tr><td><i>802.11g</i></td><td>802.11g/b.</td></tr><tr><td><i>802.11n</i></td><td>802.11n/g/b at 2.4GHz.</td></tr><tr><td><i>802.11n-5G</i></td><td>802.11n/a at 5GHz.</td></tr><tr><td><i>802.11ac</i></td><td>802.11ac/n/a.</td></tr><tr><td><i>802.11ax-5G</i></td><td>802.11ax/ac/n/a at 5GHz.</td></tr><tr><td><i>802.11ax</i></td><td>802.11ax/n/g/b at 2.4GHz.</td></tr><tr><td><i>802.11ac-2G</i></td><td>802.11ac at 2.4GHz.</td></tr><tr><td><i>802.11ax-6G</i></td><td>802.11ax at 6GHz.</td></tr><tr><td><i>802.11n,g-only</i></td><td>802.11n/g at 2.4GHz.</td></tr><tr><td><i>802.11g-only</i></td><td>802.11g.</td></tr><tr><td><i>802.11n-only</i></td><td>802.11n at 2.4GHz.</td></tr><tr><td><i>802.11n-5G-only</i></td><td>802.11n at 5GHz.</td></tr><tr><td><i>802.11ac,n-only</i></td><td>802.11ac/n.</td></tr><tr><td><i>802.11ac-only</i></td><td>802.11ac.</td></tr></table>	Option	Description	<i>802.11a</i>	802.11a.	<i>802.11b</i>	802.11b.	<i>802.11g</i>	802.11g/b.	<i>802.11n</i>	802.11n/g/b at 2.4GHz.	<i>802.11n-5G</i>	802.11n/a at 5GHz.	<i>802.11ac</i>	802.11ac/n/a.	<i>802.11ax-5G</i>	802.11ax/ac/n/a at 5GHz.	<i>802.11ax</i>	802.11ax/n/g/b at 2.4GHz.	<i>802.11ac-2G</i>	802.11ac at 2.4GHz.	<i>802.11ax-6G</i>	802.11ax at 6GHz.	<i>802.11n,g-only</i>	802.11n/g at 2.4GHz.	<i>802.11g-only</i>	802.11g.	<i>802.11n-only</i>	802.11n at 2.4GHz.	<i>802.11n-5G-only</i>	802.11n at 5GHz.	<i>802.11ac,n-only</i>	802.11ac/n.	<i>802.11ac-only</i>	802.11ac.			
Option	Description																																					
<i>802.11a</i>	802.11a.																																					
<i>802.11b</i>	802.11b.																																					
<i>802.11g</i>	802.11g/b.																																					
<i>802.11n</i>	802.11n/g/b at 2.4GHz.																																					
<i>802.11n-5G</i>	802.11n/a at 5GHz.																																					
<i>802.11ac</i>	802.11ac/n/a.																																					
<i>802.11ax-5G</i>	802.11ax/ac/n/a at 5GHz.																																					
<i>802.11ax</i>	802.11ax/n/g/b at 2.4GHz.																																					
<i>802.11ac-2G</i>	802.11ac at 2.4GHz.																																					
<i>802.11ax-6G</i>	802.11ax at 6GHz.																																					
<i>802.11n,g-only</i>	802.11n/g at 2.4GHz.																																					
<i>802.11g-only</i>	802.11g.																																					
<i>802.11n-only</i>	802.11n at 2.4GHz.																																					
<i>802.11n-5G-only</i>	802.11n at 5GHz.																																					
<i>802.11ac,n-only</i>	802.11ac/n.																																					
<i>802.11ac-only</i>	802.11ac.																																					

Parameter	Description	Type	Size	Default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>802.11ax,ac-only</td><td>802.11ax/ac at 5GHz.</td></tr><tr><td>802.11ax,ac,n-only</td><td>802.11ax/ac/n at 5GHz.</td></tr><tr><td>802.11ax-5G-only</td><td>802.11ax at 5GHz.</td></tr><tr><td>802.11ax,n-only</td><td>802.11ax/n at 2.4GHz.</td></tr><tr><td>802.11ax,n,g-only</td><td>802.11ax/n/g at 2.4GHz.</td></tr><tr><td>802.11ax-only</td><td>802.11ax at 2.4GHz.</td></tr></table>	Option	Description	802.11ax,ac-only	802.11ax/ac at 5GHz.	802.11ax,ac,n-only	802.11ax/ac/n at 5GHz.	802.11ax-5G-only	802.11ax at 5GHz.	802.11ax,n-only	802.11ax/n at 2.4GHz.	802.11ax,n,g-only	802.11ax/n/g at 2.4GHz.	802.11ax-only	802.11ax at 2.4GHz.			
	Option	Description																
	802.11ax,ac-only	802.11ax/ac at 5GHz.																
	802.11ax,ac,n-only	802.11ax/ac/n at 5GHz.																
	802.11ax-5G-only	802.11ax at 5GHz.																
	802.11ax,n-only	802.11ax/n at 2.4GHz.																
	802.11ax,n,g-only	802.11ax/n/g at 2.4GHz.																
802.11ax-only	802.11ax at 2.4GHz.																	
band-5g-type	WiFi 5G band type.	option	-	5g-full														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>5g-full</td><td>Full 5G band.</td></tr><tr><td>5g-high</td><td>High 5G band.</td></tr><tr><td>5g-low</td><td>Low 5G band.</td></tr></table>	Option	Description	5g-full	Full 5G band.	5g-high	High 5G band.	5g-low	Low 5G band.									
	Option	Description																
	5g-full	Full 5G band.																
	5g-high	High 5G band.																
5g-low	Low 5G band.																	
drma	Enable/disable dynamic radio mode assignment.	option	-	disable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>disable</td><td>Disable dynamic radio mode assignment (DRMA).</td></tr><tr><td>enable</td><td>Enable dynamic radio mode assignment (DRMA).</td></tr></table>	Option	Description	disable	Disable dynamic radio mode assignment (DRMA).	enable	Enable dynamic radio mode assignment (DRMA).											
	Option	Description																
	disable	Disable dynamic radio mode assignment (DRMA).																
enable	Enable dynamic radio mode assignment (DRMA).																	
drma-sensitivity	Network Coverage Factor.	option	-	low														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>low</td><td>Consider a radio as redundant when its NCF is 100%.</td></tr><tr><td>medium</td><td>Consider a radio as redundant when its NCF is 95%.</td></tr><tr><td>high</td><td>Consider a radio as redundant when its NCF is 90%.</td></tr></table>	Option	Description	low	Consider a radio as redundant when its NCF is 100%.	medium	Consider a radio as redundant when its NCF is 95%.	high	Consider a radio as redundant when its NCF is 90%.									
	Option	Description																
	low	Consider a radio as redundant when its NCF is 100%.																
	medium	Consider a radio as redundant when its NCF is 95%.																
high	Consider a radio as redundant when its NCF is 90%.																	
airtime-fairness	Enable/disable airtime fairness.	option	-	disable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable airtime fairness (ATF) support.</td></tr><tr><td>disable</td><td>Disable airtime fairness (ATF) support.</td></tr></table>	Option	Description	enable	Enable airtime fairness (ATF) support.	disable	Disable airtime fairness (ATF) support.											
	Option	Description																
	enable	Enable airtime fairness (ATF) support.																
disable	Disable airtime fairness (ATF) support.																	

Parameter	Description	Type	Size	Default
protection-mode	Enable/disable 802.11g protection modes to support backwards compatibility with older clients (rtscts, ctsonly, disable).	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>rtscts</i>	Enable 802.11g protection RTS/CTS mode.		
	<i>ctsonly</i>	Enable 802.11g protection CTS only mode.		
	<i>disable</i>	Disable 802.11g protection mode.		
powersave-optimize	Enable client power-saving features such as TIM, AC VO, and OBSS etc.	option	-	
	<b>Option</b>	<b>Description</b>		
	<i>tim</i>	TIM bit for client in power save mode.		
	<i>ac-vo</i>	Use AC VO priority to send out packets in the power save queue.		
	<i>no-obss-scan</i>	Do not put OBSS scan IE into beacon and probe response frames.		
	<i>no-11b-rate</i>	Do not send frame using 11b data rate.		
	<i>client-rate-follow</i>	Adapt transmitting PHY rate with receiving PHY rate from a client.		
transmit-optimize	Packet transmission optimization options including power saving, aggregation limiting, retry limiting, etc. All are enabled by default.	option	-	power-save aggr-limit retry-limit send-bar
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable packet transmission optimization.		
	<i>power-save</i>	Tag client as operating in power save mode if excessive transmit retries occur.		
	<i>aggr-limit</i>	Set aggregation limit to a lower value when data rate is low.		
	<i>retry-limit</i>	Set software retry limit to a lower value when data rate is low.		
	<i>send-bar</i>	Limit transmission of BAR frames.		
amsdu	Enable/disable 802.11n AMSDU support. AMSDU can improve performance if supported by your WiFi clients.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable AMSDU support.		
	<i>disable</i>	Disable AMSDU support.		

Parameter	Description	Type	Size	Default										
coexistence	Enable/disable allowing both HT20 and HT40 on the same radio.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable support for both HT20 and HT40 on the same radio.</td></tr><tr><td><i>disable</i></td><td>Disable support for both HT20 and HT40 on the same radio.</td></tr></table>	Option	Description	<i>enable</i>	Enable support for both HT20 and HT40 on the same radio.	<i>disable</i>	Disable support for both HT20 and HT40 on the same radio.							
Option	Description													
<i>enable</i>	Enable support for both HT20 and HT40 on the same radio.													
<i>disable</i>	Disable support for both HT20 and HT40 on the same radio.													
zero-wait-dfs	Enable/disable zero wait DFS on radio.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable zero wait DFS</td></tr><tr><td><i>disable</i></td><td>Disable zero wait DFS</td></tr></table>	Option	Description	<i>enable</i>	Enable zero wait DFS	<i>disable</i>	Disable zero wait DFS							
Option	Description													
<i>enable</i>	Enable zero wait DFS													
<i>disable</i>	Disable zero wait DFS													
bss-color	BSS color value for this 11ax radio.	integer	Minimum value: 0 Maximum value: 63	0										
bss-color-mode	BSS color mode for this 11ax radio.	option	-	auto										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto</i></td><td>Automatically select BSS color value on AP.</td></tr><tr><td><i>static</i></td><td>Set BSS color value on this radio based on 'bss-color' CLI.</td></tr></table>	Option	Description	<i>auto</i>	Automatically select BSS color value on AP.	<i>static</i>	Set BSS color value on this radio based on 'bss-color' CLI.							
Option	Description													
<i>auto</i>	Automatically select BSS color value on AP.													
<i>static</i>	Set BSS color value on this radio based on 'bss-color' CLI.													
short-guard-interval	Use either the short guard interval (Short GI) of 400 ns or the long guard interval (Long GI) of 800 ns.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Select the 400 ns short guard interval (Short GI).</td></tr><tr><td><i>disable</i></td><td>Select the 800 ns long guard interval (Long GI).</td></tr></table>	Option	Description	<i>enable</i>	Select the 400 ns short guard interval (Short GI).	<i>disable</i>	Select the 800 ns long guard interval (Long GI).							
Option	Description													
<i>enable</i>	Select the 400 ns short guard interval (Short GI).													
<i>disable</i>	Select the 800 ns long guard interval (Long GI).													
channel-bonding	Channel bandwidth: 160,80, 40, or 20MHz. Channels may use both 20 and 40 by enabling coexistence.	option	-	20MHz										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>160MHz</i></td><td>160 MHz channel width.</td></tr><tr><td><i>80MHz</i></td><td>80 MHz channel width.</td></tr><tr><td><i>40MHz</i></td><td>40 MHz channel width.</td></tr><tr><td><i>20MHz</i></td><td>20 MHz channel width.</td></tr></table>	Option	Description	<i>160MHz</i>	160 MHz channel width.	<i>80MHz</i>	80 MHz channel width.	<i>40MHz</i>	40 MHz channel width.	<i>20MHz</i>	20 MHz channel width.			
Option	Description													
<i>160MHz</i>	160 MHz channel width.													
<i>80MHz</i>	80 MHz channel width.													
<i>40MHz</i>	40 MHz channel width.													
<i>20MHz</i>	20 MHz channel width.													

Parameter	Description	Type	Size	Default						
auto-power-level	Enable/disable automatic power-level adjustment to prevent co-channel interference.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable automatic transmit power adjustment.</td></tr><tr><td><i>disable</i></td><td>Disable automatic transmit power adjustment.</td></tr></table>	Option	Description	<i>enable</i>	Enable automatic transmit power adjustment.	<i>disable</i>	Disable automatic transmit power adjustment.			
Option	Description									
<i>enable</i>	Enable automatic transmit power adjustment.									
<i>disable</i>	Disable automatic transmit power adjustment.									
auto-power-high	The upper bound of automatic transmit power adjustment in dBm (the actual range of transmit power depends on the AP platform type).	integer	Minimum value: 0 Maximum value: 4294967295	17						
auto-power-low	The lower bound of automatic transmit power adjustment in dBm (the actual range of transmit power depends on the AP platform type).	integer	Minimum value: 0 Maximum value: 4294967295	10						
auto-power-target	Target of automatic transmit power adjustment in dBm.	string	Maximum length: 7	-70						
power-mode	Set radio effective isotropic radiated power. This power takes into account both radio transmit power and antenna gain. Higher power level settings may be constrained by local regulatory requirements and AP capabilities.	option	-	percentage						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>dBm</i></td><td>Set radio EIRP power in dBm.</td></tr><tr><td><i>percentage</i></td><td>Set radio EIRP power by percentage.</td></tr></table>	Option	Description	<i>dBm</i>	Set radio EIRP power in dBm.	<i>percentage</i>	Set radio EIRP power by percentage.			
Option	Description									
<i>dBm</i>	Set radio EIRP power in dBm.									
<i>percentage</i>	Set radio EIRP power by percentage.									
power-level	Radio EIRP power level as a percentage of the maximum EIRP power.	integer	Minimum value: 0 Maximum value: 100	100						
power-value	Radio EIRP power in dBm.	integer	Minimum value: 1 Maximum value: 33	27						

Parameter	Description	Type	Size	Default						
dtim	Delivery Traffic Indication Map. Set higher to save battery life of WiFi client in power-save mode.	integer	Minimum value: 1 Maximum value: 255	1						
beacon-interval	Beacon interval. The time between beacon frames in milliseconds. Actual range of beacon interval depends on the AP platform type.	integer	Minimum value: 0 Maximum value: 65535	100						
rts-threshold	Maximum packet size for RTS transmissions, specifying the maximum size of a data packet before RTS/CTS.	integer	Minimum value: 256 Maximum value: 2346	2346						
frag-threshold	Maximum packet size that can be sent without fragmentation.	integer	Minimum value: 800 Maximum value: 2346	2346						
ap-sniffer-bufsize	Sniffer buffer size.	integer	Minimum value: 1 Maximum value: 32	16						
ap-sniffer-chan	Channel on which to operate the sniffer.	integer	Minimum value: 0 Maximum value: 4294967295	6						
ap-sniffer-addr	MAC address to monitor.	mac-address	Not Specified	00:00:00:00:00:00						
ap-sniffer-mgmt-beacon	Enable/disable sniffer on WiFi management Beacon frames.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable sniffer on WiFi management beacon frame.</td></tr><tr><td>disable</td><td>Disable sniffer on WiFi management beacon frame.</td></tr></table>				Option	Description	enable	Enable sniffer on WiFi management beacon frame.	disable	Disable sniffer on WiFi management beacon frame.
Option	Description									
enable	Enable sniffer on WiFi management beacon frame.									
disable	Disable sniffer on WiFi management beacon frame.									
ap-sniffer-mgmt-probe	Enable/disable sniffer on WiFi management probe frames.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable sniffer on WiFi management probe frame.</td></tr><tr><td>disable</td><td>Enable sniffer on WiFi management probe frame.</td></tr></table>				Option	Description	enable	Enable sniffer on WiFi management probe frame.	disable	Enable sniffer on WiFi management probe frame.
Option	Description									
enable	Enable sniffer on WiFi management probe frame.									
disable	Enable sniffer on WiFi management probe frame.									



Parameter	Description	Type	Size	Default								
ap-sniffer-mgmt-other	Enable/disable sniffer on WiFi management other frames .	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable sniffer on WiFi management other frame.</td></tr><tr><td><i>disable</i></td><td>Disable sniffer on WiFi management other frame.</td></tr></table>	Option	Description	<i>enable</i>	Enable sniffer on WiFi management other frame.	<i>disable</i>	Disable sniffer on WiFi management other frame.					
Option	Description											
<i>enable</i>	Enable sniffer on WiFi management other frame.											
<i>disable</i>	Disable sniffer on WiFi management other frame.											
ap-sniffer-ctl	Enable/disable sniffer on WiFi control frame.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable sniffer on WiFi control frame.</td></tr><tr><td><i>disable</i></td><td>Disable sniffer on WiFi control frame.</td></tr></table>	Option	Description	<i>enable</i>	Enable sniffer on WiFi control frame.	<i>disable</i>	Disable sniffer on WiFi control frame.					
Option	Description											
<i>enable</i>	Enable sniffer on WiFi control frame.											
<i>disable</i>	Disable sniffer on WiFi control frame.											
ap-sniffer-data	Enable/disable sniffer on WiFi data frame.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable sniffer on WiFi data frame</td></tr><tr><td><i>disable</i></td><td>Disable sniffer on WiFi data frame</td></tr></table>	Option	Description	<i>enable</i>	Enable sniffer on WiFi data frame	<i>disable</i>	Disable sniffer on WiFi data frame					
Option	Description											
<i>enable</i>	Enable sniffer on WiFi data frame											
<i>disable</i>	Disable sniffer on WiFi data frame											
sam-ssid	SSID for WiFi network.	string	Maximum length: 32									
sam-bssid	BSSID for WiFi network.	mac-address	Not Specified	00:00:00:00:00:00								
sam-security-type	Select WiFi network security type.	option	-	wpa-personal								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>open</i></td><td>Open.</td></tr><tr><td><i>wpa-personal</i></td><td>WPA/WPA2 personal.</td></tr><tr><td><i>wpa-enterprise</i></td><td>WPA/WPA2 enterprise.</td></tr></table>	Option	Description	<i>open</i>	Open.	<i>wpa-personal</i>	WPA/WPA2 personal.	<i>wpa-enterprise</i>	WPA/WPA2 enterprise.			
Option	Description											
<i>open</i>	Open.											
<i>wpa-personal</i>	WPA/WPA2 personal.											
<i>wpa-enterprise</i>	WPA/WPA2 enterprise.											
sam-captive-portal	Enable/disable Captive Portal Authentication.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Captive Portal Authentication.</td></tr><tr><td><i>disable</i></td><td>Disable Captive Portal Authentication.</td></tr></table>	Option	Description	<i>enable</i>	Enable Captive Portal Authentication.	<i>disable</i>	Disable Captive Portal Authentication.					
Option	Description											
<i>enable</i>	Enable Captive Portal Authentication.											
<i>disable</i>	Disable Captive Portal Authentication.											

Parameter	Description	Type	Size	Default						
sam-cwp-username	Username for captive portal authentication.	string	Maximum length: 35							
sam-cwp-password	Password for captive portal authentication.	password	Not Specified							
sam-cwp-test-url	Website the client is trying to access.	string	Maximum length: 255							
sam-cwp-match-string	Identification string from the captive portal login form.	string	Maximum length: 64							
sam-cwp-success-string	Success identification on the page after a successful login.	string	Maximum length: 64							
sam-cwp-failure-string	Failure identification on the page after an incorrect login.	string	Maximum length: 64							
sam-username	Username for WiFi network connection.	string	Maximum length: 35							
sam-password	Passphrase for WiFi network connection.	password	Not Specified							
sam-test	Select SAM test type.	option	-	ping						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ping</i></td><td>PING test.</td></tr><tr><td><i>iperf</i></td><td>IPERF test.</td></tr></table>				Option	Description	<i>ping</i>	PING test.	<i>iperf</i>	IPERF test.
Option	Description									
<i>ping</i>	PING test.									
<i>iperf</i>	IPERF test.									
sam-server-type	Select SAM server type.	option	-	ip						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ip</i></td><td>IPv4 address.</td></tr><tr><td><i>fqdn</i></td><td>Fully Qualified Domain Name address.</td></tr></table>				Option	Description	<i>ip</i>	IPv4 address.	<i>fqdn</i>	Fully Qualified Domain Name address.
Option	Description									
<i>ip</i>	IPv4 address.									
<i>fqdn</i>	Fully Qualified Domain Name address.									
sam-server-ip	SAM test server IP address.	ipv4-address	Not Specified	0.0.0.0						
sam-server-fqdn	SAM test server domain name.	string	Maximum length: 255							
iperf-server-port	Iperf service port number.	integer	Minimum value: 0 Maximum value: 65535	5001						
iperf-protocol	Iperf test protocol.	option	-	udp						

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>udp</i></td><td>UDP.</td></tr><tr><td><i>tcp</i></td><td>TCP.</td></tr></table>	Option	Description	<i>udp</i>	UDP.	<i>tcp</i>	TCP.			
	Option	Description								
	<i>udp</i>	UDP.								
<i>tcp</i>	TCP.									
sam-report-intv	SAM report interval (sec), 0 for a one-time report.	integer	Minimum value: 60 Maximum value: 864000	0						
channel-utilization	Enable/disable measuring channel utilization.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable measuring channel utilization.</td></tr><tr><td><i>disable</i></td><td>Disable measuring channel utilization.</td></tr></table>	Option	Description	<i>enable</i>	Enable measuring channel utilization.	<i>disable</i>	Disable measuring channel utilization.			
	Option	Description								
	<i>enable</i>	Enable measuring channel utilization.								
<i>disable</i>	Disable measuring channel utilization.									
wids-profile	Wireless Intrusion Detection System (WIDS) profile name to assign to the radio.	string	Maximum length: 35							
darrp	Enable/disable Distributed Automatic Radio Resource Provisioning.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable distributed automatic radio resource provisioning.</td></tr><tr><td><i>disable</i></td><td>Disable distributed automatic radio resource provisioning.</td></tr></table>	Option	Description	<i>enable</i>	Enable distributed automatic radio resource provisioning.	<i>disable</i>	Disable distributed automatic radio resource provisioning.			
	Option	Description								
	<i>enable</i>	Enable distributed automatic radio resource provisioning.								
<i>disable</i>	Disable distributed automatic radio resource provisioning.									
arrp-profile	Distributed Automatic Radio Resource Provisioning (DARRP) profile name to assign to the radio.	string	Maximum length: 35							
max-clients	Maximum number of stations (STAs) or WiFi clients supported by the radio. Range depends on the hardware.	integer	Minimum value: 0 Maximum value: 4294967295	0						
max-distance	Maximum expected distance between the AP and clients.	integer	Minimum value: 0 Maximum value: 54000	0						
vap-all	Configure method for assigning SSIDs to this FortiAP.	option	-	tunnel						

Parameter	Description	Type	Size	Default									
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>tunnel</i></td><td>Automatically select tunnel SSIDs.</td></tr><tr><td><i>bridge</i></td><td>Automatically select local-bridging SSIDs.</td></tr><tr><td><i>manual</i></td><td>Manually select SSIDs.</td></tr></table>		Option	Description	<i>tunnel</i>	Automatically select tunnel SSIDs.	<i>bridge</i>	Automatically select local-bridging SSIDs.	<i>manual</i>	Manually select SSIDs.			
	Option	Description											
	<i>tunnel</i>	Automatically select tunnel SSIDs.											
	<i>bridge</i>	Automatically select local-bridging SSIDs.											
<i>manual</i>	Manually select SSIDs.												
vaps <name>	Manually selected list of Virtual Access Points (VAPs). Virtual Access Point (VAP) name.	string	Maximum length: 35										
channel <chan>	Selected list of wireless radio channels. Channel number.	string	Maximum length: 3										
call-admission-control	Enable/disable WiFi multimedia (WMM) call admission control to optimize WiFi bandwidth use for VoIP calls. New VoIP calls are only accepted if there is enough bandwidth available to support them.	option	-	disable									
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable WMM call admission control.</td></tr><tr><td><i>disable</i></td><td>Disable WMM call admission control.</td></tr></table>		Option	Description	<i>enable</i>	Enable WMM call admission control.	<i>disable</i>	Disable WMM call admission control.					
	Option	Description											
	<i>enable</i>	Enable WMM call admission control.											
<i>disable</i>	Disable WMM call admission control.												
call-capacity	Maximum number of Voice over WLAN.	integer	Minimum value: 0 Maximum value: 60	10									
bandwidth-admission-control	Enable/disable WiFi multimedia (WMM) bandwidth admission control to optimize WiFi bandwidth use. A request to join the wireless network is only allowed if the access point has enough bandwidth to support it.	option	-	disable									
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable WMM bandwidth admission control.</td></tr><tr><td><i>disable</i></td><td>Disable WMM bandwidth admission control.</td></tr></table>		Option	Description	<i>enable</i>	Enable WMM bandwidth admission control.	<i>disable</i>	Disable WMM bandwidth admission control.					
	Option	Description											
	<i>enable</i>	Enable WMM bandwidth admission control.											
<i>disable</i>	Disable WMM bandwidth admission control.												
bandwidth-capacity	Maximum bandwidth capacity allowed.	integer	Minimum value: 1 Maximum value: 600000	2000									

## config radio-4

Parameter	Description	Type	Size	Default																																		
mode	Mode of radio 3. Radio 3 can be disabled, configured as an access point, a rogue AP monitor, a sniffer, or a station.	option	-	ap																																		
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disabled</i></td><td>Radio 3 is disabled.</td></tr><tr><td><i>ap</i></td><td>Radio 3 operates as an access point that allows WiFi clients to connect to your network.</td></tr><tr><td><i>monitor</i></td><td>Radio 3 operates as a dedicated monitor. As a monitor, the radio scans for other WiFi access points and adds them to the Rogue AP monitor list.</td></tr><tr><td><i>sniffer</i></td><td>Radio 3 operates as a sniffer capturing WiFi frames on air.</td></tr><tr><td><i>sam</i></td><td>Radio 3 operates as a station that can connect to a neighboring AP for connectivity and health check.</td></tr></table>	Option	Description	<i>disabled</i>	Radio 3 is disabled.	<i>ap</i>	Radio 3 operates as an access point that allows WiFi clients to connect to your network.	<i>monitor</i>	Radio 3 operates as a dedicated monitor. As a monitor, the radio scans for other WiFi access points and adds them to the Rogue AP monitor list.	<i>sniffer</i>	Radio 3 operates as a sniffer capturing WiFi frames on air.	<i>sam</i>	Radio 3 operates as a station that can connect to a neighboring AP for connectivity and health check.																									
Option	Description																																					
<i>disabled</i>	Radio 3 is disabled.																																					
<i>ap</i>	Radio 3 operates as an access point that allows WiFi clients to connect to your network.																																					
<i>monitor</i>	Radio 3 operates as a dedicated monitor. As a monitor, the radio scans for other WiFi access points and adds them to the Rogue AP monitor list.																																					
<i>sniffer</i>	Radio 3 operates as a sniffer capturing WiFi frames on air.																																					
<i>sam</i>	Radio 3 operates as a station that can connect to a neighboring AP for connectivity and health check.																																					
band	WiFi band that Radio 3 operates on.	option	-																																			
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>802.11a</i></td><td>802.11a.</td></tr><tr><td><i>802.11b</i></td><td>802.11b.</td></tr><tr><td><i>802.11g</i></td><td>802.11g/b.</td></tr><tr><td><i>802.11n</i></td><td>802.11n/g/b at 2.4GHz.</td></tr><tr><td><i>802.11n-5G</i></td><td>802.11n/a at 5GHz.</td></tr><tr><td><i>802.11ac</i></td><td>802.11ac/n/a.</td></tr><tr><td><i>802.11ax-5G</i></td><td>802.11ax/ac/n/a at 5GHz.</td></tr><tr><td><i>802.11ax</i></td><td>802.11ax/n/g/b at 2.4GHz.</td></tr><tr><td><i>802.11ac-2G</i></td><td>802.11ac at 2.4GHz.</td></tr><tr><td><i>802.11ax-6G</i></td><td>802.11ax at 6GHz.</td></tr><tr><td><i>802.11n,g-only</i></td><td>802.11n/g at 2.4GHz.</td></tr><tr><td><i>802.11g-only</i></td><td>802.11g.</td></tr><tr><td><i>802.11n-only</i></td><td>802.11n at 2.4GHz.</td></tr><tr><td><i>802.11n-5G-only</i></td><td>802.11n at 5GHz.</td></tr><tr><td><i>802.11ac,n-only</i></td><td>802.11ac/n.</td></tr><tr><td><i>802.11ac-only</i></td><td>802.11ac.</td></tr></table>	Option	Description	<i>802.11a</i>	802.11a.	<i>802.11b</i>	802.11b.	<i>802.11g</i>	802.11g/b.	<i>802.11n</i>	802.11n/g/b at 2.4GHz.	<i>802.11n-5G</i>	802.11n/a at 5GHz.	<i>802.11ac</i>	802.11ac/n/a.	<i>802.11ax-5G</i>	802.11ax/ac/n/a at 5GHz.	<i>802.11ax</i>	802.11ax/n/g/b at 2.4GHz.	<i>802.11ac-2G</i>	802.11ac at 2.4GHz.	<i>802.11ax-6G</i>	802.11ax at 6GHz.	<i>802.11n,g-only</i>	802.11n/g at 2.4GHz.	<i>802.11g-only</i>	802.11g.	<i>802.11n-only</i>	802.11n at 2.4GHz.	<i>802.11n-5G-only</i>	802.11n at 5GHz.	<i>802.11ac,n-only</i>	802.11ac/n.	<i>802.11ac-only</i>	802.11ac.			
Option	Description																																					
<i>802.11a</i>	802.11a.																																					
<i>802.11b</i>	802.11b.																																					
<i>802.11g</i>	802.11g/b.																																					
<i>802.11n</i>	802.11n/g/b at 2.4GHz.																																					
<i>802.11n-5G</i>	802.11n/a at 5GHz.																																					
<i>802.11ac</i>	802.11ac/n/a.																																					
<i>802.11ax-5G</i>	802.11ax/ac/n/a at 5GHz.																																					
<i>802.11ax</i>	802.11ax/n/g/b at 2.4GHz.																																					
<i>802.11ac-2G</i>	802.11ac at 2.4GHz.																																					
<i>802.11ax-6G</i>	802.11ax at 6GHz.																																					
<i>802.11n,g-only</i>	802.11n/g at 2.4GHz.																																					
<i>802.11g-only</i>	802.11g.																																					
<i>802.11n-only</i>	802.11n at 2.4GHz.																																					
<i>802.11n-5G-only</i>	802.11n at 5GHz.																																					
<i>802.11ac,n-only</i>	802.11ac/n.																																					
<i>802.11ac-only</i>	802.11ac.																																					

Parameter	Description	Type	Size	Default														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>802.11ax,ac-only</i></td><td>802.11ax/ac at 5GHz.</td></tr><tr><td><i>802.11ax,ac,n-only</i></td><td>802.11ax/ac/n at 5GHz.</td></tr><tr><td><i>802.11ax-5G-only</i></td><td>802.11ax at 5GHz.</td></tr><tr><td><i>802.11ax,n-only</i></td><td>802.11ax/n at 2.4GHz.</td></tr><tr><td><i>802.11ax,n,g-only</i></td><td>802.11ax/n/g at 2.4GHz.</td></tr><tr><td><i>802.11ax-only</i></td><td>802.11ax at 2.4GHz.</td></tr></table>	Option	Description	<i>802.11ax,ac-only</i>	802.11ax/ac at 5GHz.	<i>802.11ax,ac,n-only</i>	802.11ax/ac/n at 5GHz.	<i>802.11ax-5G-only</i>	802.11ax at 5GHz.	<i>802.11ax,n-only</i>	802.11ax/n at 2.4GHz.	<i>802.11ax,n,g-only</i>	802.11ax/n/g at 2.4GHz.	<i>802.11ax-only</i>	802.11ax at 2.4GHz.			
	Option	Description																
	<i>802.11ax,ac-only</i>	802.11ax/ac at 5GHz.																
	<i>802.11ax,ac,n-only</i>	802.11ax/ac/n at 5GHz.																
	<i>802.11ax-5G-only</i>	802.11ax at 5GHz.																
	<i>802.11ax,n-only</i>	802.11ax/n at 2.4GHz.																
	<i>802.11ax,n,g-only</i>	802.11ax/n/g at 2.4GHz.																
<i>802.11ax-only</i>	802.11ax at 2.4GHz.																	
band-5g-type	WiFi 5G band type.	option	-	5g-full														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>5g-full</i></td><td>Full 5G band.</td></tr><tr><td><i>5g-high</i></td><td>High 5G band.</td></tr><tr><td><i>5g-low</i></td><td>Low 5G band.</td></tr></table>	Option	Description	<i>5g-full</i>	Full 5G band.	<i>5g-high</i>	High 5G band.	<i>5g-low</i>	Low 5G band.									
	Option	Description																
	<i>5g-full</i>	Full 5G band.																
	<i>5g-high</i>	High 5G band.																
<i>5g-low</i>	Low 5G band.																	
drma	Enable/disable dynamic radio mode assignment.	option	-	disable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Disable dynamic radio mode assignment (DRMA).</td></tr><tr><td><i>enable</i></td><td>Enable dynamic radio mode assignment (DRMA).</td></tr></table>	Option	Description	<i>disable</i>	Disable dynamic radio mode assignment (DRMA).	<i>enable</i>	Enable dynamic radio mode assignment (DRMA).											
	Option	Description																
	<i>disable</i>	Disable dynamic radio mode assignment (DRMA).																
<i>enable</i>	Enable dynamic radio mode assignment (DRMA).																	
drma-sensitivity	Network Coverage Factor.	option	-	low														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>low</i></td><td>Consider a radio as redundant when its NCF is 100%.</td></tr><tr><td><i>medium</i></td><td>Consider a radio as redundant when its NCF is 95%.</td></tr><tr><td><i>high</i></td><td>Consider a radio as redundant when its NCF is 90%.</td></tr></table>	Option	Description	<i>low</i>	Consider a radio as redundant when its NCF is 100%.	<i>medium</i>	Consider a radio as redundant when its NCF is 95%.	<i>high</i>	Consider a radio as redundant when its NCF is 90%.									
	Option	Description																
	<i>low</i>	Consider a radio as redundant when its NCF is 100%.																
	<i>medium</i>	Consider a radio as redundant when its NCF is 95%.																
<i>high</i>	Consider a radio as redundant when its NCF is 90%.																	
airtime-fairness	Enable/disable airtime fairness.	option	-	disable														
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable airtime fairness (ATF) support.</td></tr><tr><td><i>disable</i></td><td>Disable airtime fairness (ATF) support.</td></tr></table>	Option	Description	<i>enable</i>	Enable airtime fairness (ATF) support.	<i>disable</i>	Disable airtime fairness (ATF) support.											
	Option	Description																
	<i>enable</i>	Enable airtime fairness (ATF) support.																
<i>disable</i>	Disable airtime fairness (ATF) support.																	

Parameter	Description	Type	Size	Default
protection-mode	Enable/disable 802.11g protection modes to support backwards compatibility with older clients (rtscts, ctsonly, disable).	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>rtscts</i>	Enable 802.11g protection RTS/CTS mode.		
	<i>ctsonly</i>	Enable 802.11g protection CTS only mode.		
	<i>disable</i>	Disable 802.11g protection mode.		
powersave-optimize	Enable client power-saving features such as TIM, AC VO, and OBSS etc.	option	-	
	<b>Option</b>	<b>Description</b>		
	<i>tim</i>	TIM bit for client in power save mode.		
	<i>ac-vo</i>	Use AC VO priority to send out packets in the power save queue.		
	<i>no-obss-scan</i>	Do not put OBSS scan IE into beacon and probe response frames.		
	<i>no-11b-rate</i>	Do not send frame using 11b data rate.		
	<i>client-rate-follow</i>	Adapt transmitting PHY rate with receiving PHY rate from a client.		
transmit-optimize	Packet transmission optimization options including power saving, aggregation limiting, retry limiting, etc. All are enabled by default.	option	-	power-save aggr-limit retry-limit send-bar
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable packet transmission optimization.		
	<i>power-save</i>	Tag client as operating in power save mode if excessive transmit retries occur.		
	<i>aggr-limit</i>	Set aggregation limit to a lower value when data rate is low.		
	<i>retry-limit</i>	Set software retry limit to a lower value when data rate is low.		
	<i>send-bar</i>	Limit transmission of BAR frames.		
amsdu	Enable/disable 802.11n AMSDU support. AMSDU can improve performance if supported by your WiFi clients.	option	-	enable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable AMSDU support.		
	<i>disable</i>	Disable AMSDU support.		

Parameter	Description	Type	Size	Default										
coexistence	Enable/disable allowing both HT20 and HT40 on the same radio.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable support for both HT20 and HT40 on the same radio.</td></tr><tr><td><i>disable</i></td><td>Disable support for both HT20 and HT40 on the same radio.</td></tr></table>	Option	Description	<i>enable</i>	Enable support for both HT20 and HT40 on the same radio.	<i>disable</i>	Disable support for both HT20 and HT40 on the same radio.							
Option	Description													
<i>enable</i>	Enable support for both HT20 and HT40 on the same radio.													
<i>disable</i>	Disable support for both HT20 and HT40 on the same radio.													
zero-wait-dfs	Enable/disable zero wait DFS on radio.	option	-	enable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable zero wait DFS</td></tr><tr><td><i>disable</i></td><td>Disable zero wait DFS</td></tr></table>	Option	Description	<i>enable</i>	Enable zero wait DFS	<i>disable</i>	Disable zero wait DFS							
Option	Description													
<i>enable</i>	Enable zero wait DFS													
<i>disable</i>	Disable zero wait DFS													
bss-color	BSS color value for this 11ax radio.	integer	Minimum value: 0 Maximum value: 63	0										
bss-color-mode	BSS color mode for this 11ax radio.	option	-	auto										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>auto</i></td><td>Automatically select BSS color value on AP.</td></tr><tr><td><i>static</i></td><td>Set BSS color value on this radio based on 'bss-color' CLI.</td></tr></table>	Option	Description	<i>auto</i>	Automatically select BSS color value on AP.	<i>static</i>	Set BSS color value on this radio based on 'bss-color' CLI.							
Option	Description													
<i>auto</i>	Automatically select BSS color value on AP.													
<i>static</i>	Set BSS color value on this radio based on 'bss-color' CLI.													
short-guard-interval	Use either the short guard interval (Short GI) of 400 ns or the long guard interval (Long GI) of 800 ns.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Select the 400 ns short guard interval (Short GI).</td></tr><tr><td><i>disable</i></td><td>Select the 800 ns long guard interval (Long GI).</td></tr></table>	Option	Description	<i>enable</i>	Select the 400 ns short guard interval (Short GI).	<i>disable</i>	Select the 800 ns long guard interval (Long GI).							
Option	Description													
<i>enable</i>	Select the 400 ns short guard interval (Short GI).													
<i>disable</i>	Select the 800 ns long guard interval (Long GI).													
channel-bonding	Channel bandwidth: 160,80, 40, or 20MHz. Channels may use both 20 and 40 by enabling coexistence.	option	-	20MHz										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>160MHz</i></td><td>160 MHz channel width.</td></tr><tr><td><i>80MHz</i></td><td>80 MHz channel width.</td></tr><tr><td><i>40MHz</i></td><td>40 MHz channel width.</td></tr><tr><td><i>20MHz</i></td><td>20 MHz channel width.</td></tr></table>	Option	Description	<i>160MHz</i>	160 MHz channel width.	<i>80MHz</i>	80 MHz channel width.	<i>40MHz</i>	40 MHz channel width.	<i>20MHz</i>	20 MHz channel width.			
Option	Description													
<i>160MHz</i>	160 MHz channel width.													
<i>80MHz</i>	80 MHz channel width.													
<i>40MHz</i>	40 MHz channel width.													
<i>20MHz</i>	20 MHz channel width.													



Parameter	Description	Type	Size	Default						
auto-power-level	Enable/disable automatic power-level adjustment to prevent co-channel interference.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable automatic transmit power adjustment.</td></tr><tr><td><i>disable</i></td><td>Disable automatic transmit power adjustment.</td></tr></table>	Option	Description	<i>enable</i>	Enable automatic transmit power adjustment.	<i>disable</i>	Disable automatic transmit power adjustment.			
Option	Description									
<i>enable</i>	Enable automatic transmit power adjustment.									
<i>disable</i>	Disable automatic transmit power adjustment.									
auto-power-high	The upper bound of automatic transmit power adjustment in dBm (the actual range of transmit power depends on the AP platform type).	integer	Minimum value: 0 Maximum value: 4294967295	17						
auto-power-low	The lower bound of automatic transmit power adjustment in dBm (the actual range of transmit power depends on the AP platform type).	integer	Minimum value: 0 Maximum value: 4294967295	10						
auto-power-target	Target of automatic transmit power adjustment in dBm.	string	Maximum length: 7	-70						
power-mode	Set radio effective isotropic radiated power. This power takes into account both radio transmit power and antenna gain. Higher power level settings may be constrained by local regulatory requirements and AP capabilities.	option	-	percentage						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>dBm</i></td><td>Set radio EIRP power in dBm.</td></tr><tr><td><i>percentage</i></td><td>Set radio EIRP power by percentage.</td></tr></table>	Option	Description	<i>dBm</i>	Set radio EIRP power in dBm.	<i>percentage</i>	Set radio EIRP power by percentage.			
Option	Description									
<i>dBm</i>	Set radio EIRP power in dBm.									
<i>percentage</i>	Set radio EIRP power by percentage.									
power-level	Radio EIRP power level as a percentage of the maximum EIRP power.	integer	Minimum value: 0 Maximum value: 100	100						
power-value	Radio EIRP power in dBm.	integer	Minimum value: 1 Maximum value: 33	27						

Parameter	Description	Type	Size	Default						
dtim	Delivery Traffic Indication Map. Set higher to save battery life of WiFi client in power-save mode.	integer	Minimum value: 1 Maximum value: 255	1						
beacon-interval	Beacon interval. The time between beacon frames in milliseconds. Actual range of beacon interval depends on the AP platform type.	integer	Minimum value: 0 Maximum value: 65535	100						
rts-threshold	Maximum packet size for RTS transmissions, specifying the maximum size of a data packet before RTS/CTS.	integer	Minimum value: 256 Maximum value: 2346	2346						
frag-threshold	Maximum packet size that can be sent without fragmentation.	integer	Minimum value: 800 Maximum value: 2346	2346						
ap-sniffer-bufsize	Sniffer buffer size.	integer	Minimum value: 1 Maximum value: 32	16						
ap-sniffer-chan	Channel on which to operate the sniffer.	integer	Minimum value: 0 Maximum value: 4294967295	6						
ap-sniffer-addr	MAC address to monitor.	mac-address	Not Specified	00:00:00:00:00:00						
ap-sniffer-mgmt-beacon	Enable/disable sniffer on WiFi management Beacon frames.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable sniffer on WiFi management beacon frame.</td></tr><tr><td>disable</td><td>Disable sniffer on WiFi management beacon frame.</td></tr></table>				Option	Description	enable	Enable sniffer on WiFi management beacon frame.	disable	Disable sniffer on WiFi management beacon frame.
Option	Description									
enable	Enable sniffer on WiFi management beacon frame.									
disable	Disable sniffer on WiFi management beacon frame.									
ap-sniffer-mgmt-probe	Enable/disable sniffer on WiFi management probe frames.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Enable sniffer on WiFi management probe frame.</td></tr><tr><td>disable</td><td>Enable sniffer on WiFi management probe frame.</td></tr></table>				Option	Description	enable	Enable sniffer on WiFi management probe frame.	disable	Enable sniffer on WiFi management probe frame.
Option	Description									
enable	Enable sniffer on WiFi management probe frame.									
disable	Enable sniffer on WiFi management probe frame.									

Parameter	Description	Type	Size	Default								
ap-sniffer-mgmt-other	Enable/disable sniffer on WiFi management other frames .	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable sniffer on WiFi management other frame.</td></tr><tr><td><i>disable</i></td><td>Disable sniffer on WiFi management other frame.</td></tr></table>	Option	Description	<i>enable</i>	Enable sniffer on WiFi management other frame.	<i>disable</i>	Disable sniffer on WiFi management other frame.					
Option	Description											
<i>enable</i>	Enable sniffer on WiFi management other frame.											
<i>disable</i>	Disable sniffer on WiFi management other frame.											
ap-sniffer-ctl	Enable/disable sniffer on WiFi control frame.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable sniffer on WiFi control frame.</td></tr><tr><td><i>disable</i></td><td>Disable sniffer on WiFi control frame.</td></tr></table>	Option	Description	<i>enable</i>	Enable sniffer on WiFi control frame.	<i>disable</i>	Disable sniffer on WiFi control frame.					
Option	Description											
<i>enable</i>	Enable sniffer on WiFi control frame.											
<i>disable</i>	Disable sniffer on WiFi control frame.											
ap-sniffer-data	Enable/disable sniffer on WiFi data frame.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable sniffer on WiFi data frame</td></tr><tr><td><i>disable</i></td><td>Disable sniffer on WiFi data frame</td></tr></table>	Option	Description	<i>enable</i>	Enable sniffer on WiFi data frame	<i>disable</i>	Disable sniffer on WiFi data frame					
Option	Description											
<i>enable</i>	Enable sniffer on WiFi data frame											
<i>disable</i>	Disable sniffer on WiFi data frame											
sam-ssid	SSID for WiFi network.	string	Maximum length: 32									
sam-bssid	BSSID for WiFi network.	mac-address	Not Specified	00:00:00:00:00:00								
sam-security-type	Select WiFi network security type.	option	-	wpa-personal								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>open</i></td><td>Open.</td></tr><tr><td><i>wpa-personal</i></td><td>WPA/WPA2 personal.</td></tr><tr><td><i>wpa-enterprise</i></td><td>WPA/WPA2 enterprise.</td></tr></table>	Option	Description	<i>open</i>	Open.	<i>wpa-personal</i>	WPA/WPA2 personal.	<i>wpa-enterprise</i>	WPA/WPA2 enterprise.			
Option	Description											
<i>open</i>	Open.											
<i>wpa-personal</i>	WPA/WPA2 personal.											
<i>wpa-enterprise</i>	WPA/WPA2 enterprise.											
sam-captive-portal	Enable/disable Captive Portal Authentication.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable Captive Portal Authentication.</td></tr><tr><td><i>disable</i></td><td>Disable Captive Portal Authentication.</td></tr></table>	Option	Description	<i>enable</i>	Enable Captive Portal Authentication.	<i>disable</i>	Disable Captive Portal Authentication.					
Option	Description											
<i>enable</i>	Enable Captive Portal Authentication.											
<i>disable</i>	Disable Captive Portal Authentication.											

Parameter	Description	Type	Size	Default						
sam-cwp-username	Username for captive portal authentication.	string	Maximum length: 35							
sam-cwp-password	Password for captive portal authentication.	password	Not Specified							
sam-cwp-test-url	Website the client is trying to access.	string	Maximum length: 255							
sam-cwp-match-string	Identification string from the captive portal login form.	string	Maximum length: 64							
sam-cwp-success-string	Success identification on the page after a successful login.	string	Maximum length: 64							
sam-cwp-failure-string	Failure identification on the page after an incorrect login.	string	Maximum length: 64							
sam-username	Username for WiFi network connection.	string	Maximum length: 35							
sam-password	Passphrase for WiFi network connection.	password	Not Specified							
sam-test	Select SAM test type.	option	-	ping						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ping</i></td><td>PING test.</td></tr><tr><td><i>iperf</i></td><td>IPERF test.</td></tr></table>				Option	Description	<i>ping</i>	PING test.	<i>iperf</i>	IPERF test.
Option	Description									
<i>ping</i>	PING test.									
<i>iperf</i>	IPERF test.									
sam-server-type	Select SAM server type.	option	-	ip						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>ip</i></td><td>IPv4 address.</td></tr><tr><td><i>fqdn</i></td><td>Fully Qualified Domain Name address.</td></tr></table>				Option	Description	<i>ip</i>	IPv4 address.	<i>fqdn</i>	Fully Qualified Domain Name address.
Option	Description									
<i>ip</i>	IPv4 address.									
<i>fqdn</i>	Fully Qualified Domain Name address.									
sam-server-ip	SAM test server IP address.	ipv4-address	Not Specified	0.0.0.0						
sam-server-fqdn	SAM test server domain name.	string	Maximum length: 255							
iperf-server-port	Iperf service port number.	integer	Minimum value: 0 Maximum value: 65535	5001						
iperf-protocol	Iperf test protocol.	option	-	udp						

Parameter	Description	Type	Size	Default						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>udp</i></td><td>UDP.</td></tr><tr><td><i>tcp</i></td><td>TCP.</td></tr></table>	Option	Description	<i>udp</i>	UDP.	<i>tcp</i>	TCP.			
	Option	Description								
	<i>udp</i>	UDP.								
<i>tcp</i>	TCP.									
sam-report-intv	SAM report interval (sec), 0 for a one-time report.	integer	Minimum value: 60 Maximum value: 864000	0						
channel-utilization	Enable/disable measuring channel utilization.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable measuring channel utilization.</td></tr><tr><td><i>disable</i></td><td>Disable measuring channel utilization.</td></tr></table>	Option	Description	<i>enable</i>	Enable measuring channel utilization.	<i>disable</i>	Disable measuring channel utilization.			
	Option	Description								
	<i>enable</i>	Enable measuring channel utilization.								
<i>disable</i>	Disable measuring channel utilization.									
wids-profile	Wireless Intrusion Detection System (WIDS) profile name to assign to the radio.	string	Maximum length: 35							
darrp	Enable/disable Distributed Automatic Radio Resource Provisioning.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable distributed automatic radio resource provisioning.</td></tr><tr><td><i>disable</i></td><td>Disable distributed automatic radio resource provisioning.</td></tr></table>	Option	Description	<i>enable</i>	Enable distributed automatic radio resource provisioning.	<i>disable</i>	Disable distributed automatic radio resource provisioning.			
	Option	Description								
	<i>enable</i>	Enable distributed automatic radio resource provisioning.								
<i>disable</i>	Disable distributed automatic radio resource provisioning.									
arrp-profile	Distributed Automatic Radio Resource Provisioning (DARRP) profile name to assign to the radio.	string	Maximum length: 35							
max-clients	Maximum number of stations (STAs) or WiFi clients supported by the radio. Range depends on the hardware.	integer	Minimum value: 0 Maximum value: 4294967295	0						
max-distance	Maximum expected distance between the AP and clients.	integer	Minimum value: 0 Maximum value: 54000	0						
vap-all	Configure method for assigning SSIDs to this FortiAP.	option	-	tunnel						

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>tunnel</i></td><td>Automatically select tunnel SSIDs.</td></tr><tr><td><i>bridge</i></td><td>Automatically select local-bridging SSIDs.</td></tr><tr><td><i>manual</i></td><td>Manually select SSIDs.</td></tr></table>	Option	Description	<i>tunnel</i>	Automatically select tunnel SSIDs.	<i>bridge</i>	Automatically select local-bridging SSIDs.	<i>manual</i>	Manually select SSIDs.			
	Option	Description										
	<i>tunnel</i>	Automatically select tunnel SSIDs.										
	<i>bridge</i>	Automatically select local-bridging SSIDs.										
<i>manual</i>	Manually select SSIDs.											
vaps <name>	Manually selected list of Virtual Access Points (VAPs). Virtual Access Point (VAP) name.	string	Maximum length: 35									
channel <chan>	Selected list of wireless radio channels. Channel number.	string	Maximum length: 3									
call-admission-control	Enable/disable WiFi multimedia (WMM) call admission control to optimize WiFi bandwidth use for VoIP calls. New VoIP calls are only accepted if there is enough bandwidth available to support them.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable WMM call admission control.</td></tr><tr><td><i>disable</i></td><td>Disable WMM call admission control.</td></tr></table>	Option	Description	<i>enable</i>	Enable WMM call admission control.	<i>disable</i>	Disable WMM call admission control.					
	Option	Description										
	<i>enable</i>	Enable WMM call admission control.										
<i>disable</i>	Disable WMM call admission control.											
call-capacity	Maximum number of Voice over WLAN.	integer	Minimum value: 0 Maximum value: 60	10								
bandwidth-admission-control	Enable/disable WiFi multimedia (WMM) bandwidth admission control to optimize WiFi bandwidth use. A request to join the wireless network is only allowed if the access point has enough bandwidth to support it.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable WMM bandwidth admission control.</td></tr><tr><td><i>disable</i></td><td>Disable WMM bandwidth admission control.</td></tr></table>	Option	Description	<i>enable</i>	Enable WMM bandwidth admission control.	<i>disable</i>	Disable WMM bandwidth admission control.					
	Option	Description										
	<i>enable</i>	Enable WMM bandwidth admission control.										
<i>disable</i>	Disable WMM bandwidth admission control.											
bandwidth-capacity	Maximum bandwidth capacity allowed.	integer	Minimum value: 1 Maximum value: 600000	2000								

## config split-tunneling-acl

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
dest-ip	Destination IP and mask for the split-tunneling subnet.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0

## config wireless-controller wtp

Configure Wireless Termination Points (WTPs), that is, FortiAPs or APs to be managed by FortiGate.

```
config wireless-controller wtp
  Description: Configure Wireless Termination Points (WTPs), that is, FortiAPs or APs to
  be managed by FortiGate.
  edit <wtp-id>
    set admin [discovered|disable|...]
    set allowaccess {option1}, {option2}, ...
    set apcfg-profile {string}
    set bonjour-profile {string}
    set coordinate-latitude {string}
    set coordinate-longitude {string}
    set firmware-provision {string}
    set firmware-provision-latest [disable|once]
    set image-download [enable|disable]
    set index {integer}
    set ip-fragment-preventing {option1}, {option2}, ...
  config lan
    Description: WTP LAN port mapping.
    set port-mode [offline|nat-to-wan|...]
    set port-ssid {string}
    set port1-mode [offline|nat-to-wan|...]
    set port1-ssid {string}
    set port2-mode [offline|nat-to-wan|...]
    set port2-ssid {string}
    set port3-mode [offline|nat-to-wan|...]
    set port3-ssid {string}
    set port4-mode [offline|nat-to-wan|...]
    set port4-ssid {string}
    set port5-mode [offline|nat-to-wan|...]
    set port5-ssid {string}
    set port6-mode [offline|nat-to-wan|...]
    set port6-ssid {string}
    set port7-mode [offline|nat-to-wan|...]
    set port7-ssid {string}
    set port8-mode [offline|nat-to-wan|...]
    set port8-ssid {string}
    set port-esl-mode [offline|nat-to-wan|...]
    set port-esl-ssid {string}
```

```

end
set led-state [enable|disable]
set location {string}
set login-passwd {password}
set login-passwd-change [yes|default|...]
set mesh-bridge-enable [default|enable|...]
set name {string}
set override-allowaccess [enable|disable]
set override-ip-fragment [enable|disable]
set override-lan [enable|disable]
set override-led-state [enable|disable]
set override-login-password-change [enable|disable]
set override-split-tunnel [enable|disable]
set override-wan-port-mode [enable|disable]
config radio-1
    Description: Configuration options for radio 1.
    set override-band [enable|disable]
    set band [802.11a|802.11b|...]
    set override-txpower [enable|disable]
    set auto-power-level [enable|disable]
    set auto-power-high {integer}
    set auto-power-low {integer}
    set auto-power-target {string}
    set power-mode [dBm|percentage]
    set power-level {integer}
    set power-value {integer}
    set override-vaps [enable|disable]
    set vap-all [tunnel|bridge|...]
    set vaps <name1>, <name2>, ...
    set override-channel [enable|disable]
    set channel <chan1>, <chan2>, ...
    set drma-manual-mode [ap|monitor|...]
end
config radio-2
    Description: Configuration options for radio 2.
    set override-band [enable|disable]
    set band [802.11a|802.11b|...]
    set override-txpower [enable|disable]
    set auto-power-level [enable|disable]
    set auto-power-high {integer}
    set auto-power-low {integer}
    set auto-power-target {string}
    set power-mode [dBm|percentage]
    set power-level {integer}
    set power-value {integer}
    set override-vaps [enable|disable]
    set vap-all [tunnel|bridge|...]
    set vaps <name1>, <name2>, ...
    set override-channel [enable|disable]
    set channel <chan1>, <chan2>, ...
    set drma-manual-mode [ap|monitor|...]
end
config radio-3
    Description: Configuration options for radio 3.
    set override-band [enable|disable]
    set band [802.11a|802.11b|...]

```



```

        set override-txpower [enable|disable]
        set auto-power-level [enable|disable]
        set auto-power-high {integer}
        set auto-power-low {integer}
        set auto-power-target {string}
        set power-mode [dBm|percentage]
        set power-level {integer}
        set power-value {integer}
        set override-vaps [enable|disable]
        set vap-all [tunnel|bridge|...]
        set vaps <name1>, <name2>, ...
        set override-channel [enable|disable]
        set channel <chan1>, <chan2>, ...
        set drma-manual-mode [ap|monitor|...]
    end
    config radio-4
        Description: Configuration options for radio 4.
        set override-band [enable|disable]
        set band [802.11a|802.11b|...]
        set override-txpower [enable|disable]
        set auto-power-level [enable|disable]
        set auto-power-high {integer}
        set auto-power-low {integer}
        set auto-power-target {string}
        set power-mode [dBm|percentage]
        set power-level {integer}
        set power-value {integer}
        set override-vaps [enable|disable]
        set vap-all [tunnel|bridge|...]
        set vaps <name1>, <name2>, ...
        set override-channel [enable|disable]
        set channel <chan1>, <chan2>, ...
        set drma-manual-mode [ap|monitor|...]
    end
    set region {string}
    set region-x {string}
    set region-y {string}
    config split-tunneling-acl
        Description: Split tunneling ACL filter list.
        edit <id>
            set dest-ip {ipv4-classnet}
        next
    end
    set split-tunneling-acl-local-ap-subnet [enable|disable]
    set split-tunneling-acl-path [tunnel|local]
    set tun-mtu-downlink {integer}
    set tun-mtu-uplink {integer}
    set uuid {uuid}
    set wan-port-mode [wan-lan|wan-only]
    set wtp-profile {string}
next
end

```

## config wireless-controller wtp

Parameter	Description	Type	Size	Default								
admin	Configure how the FortiGate operating as a wireless controller discovers and manages this WTP, AP or FortiAP.	option	-	enable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>discovered</i></td><td>FortiGate wireless controller discovers the WTP, AP, or FortiAP though discovery or join request messages.</td></tr><tr><td><i>disable</i></td><td>FortiGate wireless controller is configured to not provide service to this WTP.</td></tr><tr><td><i>enable</i></td><td>FortiGate wireless controller is configured to provide service to this WTP.</td></tr></table>	Option	Description	<i>discovered</i>	FortiGate wireless controller discovers the WTP, AP, or FortiAP though discovery or join request messages.	<i>disable</i>	FortiGate wireless controller is configured to not provide service to this WTP.	<i>enable</i>	FortiGate wireless controller is configured to provide service to this WTP.			
Option	Description											
<i>discovered</i>	FortiGate wireless controller discovers the WTP, AP, or FortiAP though discovery or join request messages.											
<i>disable</i>	FortiGate wireless controller is configured to not provide service to this WTP.											
<i>enable</i>	FortiGate wireless controller is configured to provide service to this WTP.											
allowaccess	Control management access to the managed WTP, FortiAP, or AP. Separate entries with a space.	option	-									
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>https</i></td><td>HTTPS access.</td></tr><tr><td><i>ssh</i></td><td>SSH access.</td></tr><tr><td><i>snmp</i></td><td>SNMP access.</td></tr></table>	Option	Description	<i>https</i>	HTTPS access.	<i>ssh</i>	SSH access.	<i>snmp</i>	SNMP access.			
Option	Description											
<i>https</i>	HTTPS access.											
<i>ssh</i>	SSH access.											
<i>snmp</i>	SNMP access.											
apcfg-profile	AP local configuration profile name.	string	Maximum length: 35									
bonjour-profile	Bonjour profile name.	string	Maximum length: 35									
coordinate-latitude	WTP latitude coordinate.	string	Maximum length: 19									
coordinate-longitude	WTP longitude coordinate.	string	Maximum length: 19									
firmware-provision	Firmware version to provision to this FortiAP on bootup (major.minor.build, i.e. 6.2.1234).	string	Maximum length: 35									
firmware-provision-latest	Enable/disable one-time automatic provisioning of the latest firmware version.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>disable</i></td><td>Do not automatically provision the latest available firmware.</td></tr><tr><td><i>once</i></td><td>Automatically attempt a one-time upgrade to the latest available firmware version.</td></tr></table>	Option	Description	<i>disable</i>	Do not automatically provision the latest available firmware.	<i>once</i>	Automatically attempt a one-time upgrade to the latest available firmware version.					
Option	Description											
<i>disable</i>	Do not automatically provision the latest available firmware.											
<i>once</i>	Automatically attempt a one-time upgrade to the latest available firmware version.											

Parameter	Description	Type	Size	Default						
image-download	Enable/disable WTP image download.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Enable WTP image download at join time.</td></tr><tr><td><i>disable</i></td><td>Disable WTP image download at join time.</td></tr></table>	Option	Description	<i>enable</i>	Enable WTP image download at join time.	<i>disable</i>	Disable WTP image download at join time.			
Option	Description									
<i>enable</i>	Enable WTP image download at join time.									
<i>disable</i>	Disable WTP image download at join time.									
index	Index.	integer	Minimum value: 0 Maximum value: 4294967295	0						
ip-fragment-preventing	Method.	option	-	tcp-mss-adjust						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>tcp-mss-adjust</i></td><td>TCP maximum segment size adjustment.</td></tr><tr><td><i>icmp-unreachable</i></td><td>Drop packet and send ICMP Destination Unreachable</td></tr></table>	Option	Description	<i>tcp-mss-adjust</i>	TCP maximum segment size adjustment.	<i>icmp-unreachable</i>	Drop packet and send ICMP Destination Unreachable			
Option	Description									
<i>tcp-mss-adjust</i>	TCP maximum segment size adjustment.									
<i>icmp-unreachable</i>	Drop packet and send ICMP Destination Unreachable									
led-state	Enable to allow the FortiAPs LEDs to light. Disable to keep the LEDs off. You may want to keep the LEDs off so they are not distracting in low light areas etc.	option	-	enable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Allow the LEDs on this FortiAP to light.</td></tr><tr><td><i>disable</i></td><td>Keep the LEDs on this FortiAP off.</td></tr></table>	Option	Description	<i>enable</i>	Allow the LEDs on this FortiAP to light.	<i>disable</i>	Keep the LEDs on this FortiAP off.			
Option	Description									
<i>enable</i>	Allow the LEDs on this FortiAP to light.									
<i>disable</i>	Keep the LEDs on this FortiAP off.									
location	Field for describing the physical location of the WTP, AP or FortiAP.	string	Maximum length: 35							
login-passwd	Set the managed WTP, FortiAP, or AP's administrator password.	password	Not Specified							
login-passwd-change	Change or reset the administrator password of a managed WTP, FortiAP or AP.	option	-	no						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>yes</i></td><td>Change the managed WTP, FortiAP or AP's administrator password. Use the login-password option to set the password.</td></tr></table>	Option	Description	<i>yes</i>	Change the managed WTP, FortiAP or AP's administrator password. Use the login-password option to set the password.					
Option	Description									
<i>yes</i>	Change the managed WTP, FortiAP or AP's administrator password. Use the login-password option to set the password.									

Parameter	Description	Type	Size	Default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>default</td><td>Keep the managed WTP, FortiAP or AP's administrator password set to the factory default.</td></tr><tr><td>no</td><td>Do not change the managed WTP, FortiAP or AP's administrator password.</td></tr></table>	Option	Description	default	Keep the managed WTP, FortiAP or AP's administrator password set to the factory default.	no	Do not change the managed WTP, FortiAP or AP's administrator password.					
	Option	Description										
	default	Keep the managed WTP, FortiAP or AP's administrator password set to the factory default.										
no	Do not change the managed WTP, FortiAP or AP's administrator password.											
mesh-bridge-enable	Enable/disable mesh Ethernet bridge when WTP is configured as a mesh branch/leaf AP.	option	-	default								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>default</td><td>Use mesh Ethernet bridge local setting on the WTP.</td></tr><tr><td>enable</td><td>Turn on mesh Ethernet bridge on the WTP.</td></tr><tr><td>disable</td><td>Turn off mesh Ethernet bridge on the WTP.</td></tr></table>	Option	Description	default	Use mesh Ethernet bridge local setting on the WTP.	enable	Turn on mesh Ethernet bridge on the WTP.	disable	Turn off mesh Ethernet bridge on the WTP.			
	Option	Description										
	default	Use mesh Ethernet bridge local setting on the WTP.										
	enable	Turn on mesh Ethernet bridge on the WTP.										
disable	Turn off mesh Ethernet bridge on the WTP.											
name	WTP, AP or FortiAP configuration name.	string	Maximum length: 35									
override-allowaccess	Enable to override the WTP profile management access configuration.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Override the WTP profile management access configuration.</td></tr><tr><td>disable</td><td>Use the WTP profile management access configuration.</td></tr></table>	Option	Description	enable	Override the WTP profile management access configuration.	disable	Use the WTP profile management access configuration.					
	Option	Description										
	enable	Override the WTP profile management access configuration.										
disable	Use the WTP profile management access configuration.											
override-ip-fragment	Enable/disable overriding the WTP profile IP fragment prevention setting.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Override the WTP profile IP fragment prevention setting.</td></tr><tr><td>disable</td><td>Use the WTP profile IP fragment prevention setting.</td></tr></table>	Option	Description	enable	Override the WTP profile IP fragment prevention setting.	disable	Use the WTP profile IP fragment prevention setting.					
	Option	Description										
	enable	Override the WTP profile IP fragment prevention setting.										
disable	Use the WTP profile IP fragment prevention setting.											
override-lan	Enable to override the WTP profile LAN port setting.	option	-	disable								
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Override the WTP profile LAN port setting.</td></tr><tr><td>disable</td><td>Use the WTP profile LAN port setting.</td></tr></table>	Option	Description	enable	Override the WTP profile LAN port setting.	disable	Use the WTP profile LAN port setting.					
	Option	Description										
	enable	Override the WTP profile LAN port setting.										
disable	Use the WTP profile LAN port setting.											
override-led-state	Enable to override the profile LED state setting for this FortiAP. You must enable this option to use the led-state command to turn off the FortiAP's LEDs.	option	-	disable								

Parameter	Description	Type	Size	Default
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Override the WTP profile LED state.		
	<i>disable</i>	Use the WTP profile LED state.		
override-login-passwd-change	Enable to override the WTP profile login-password (administrator password) setting.	option	-	disable
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Override the WTP profile login-password (administrator password) setting.		
	<i>disable</i>	Use the the WTP profile login-password (administrator password) setting.		
override-split-tunnel	Enable/disable overriding the WTP profile split tunneling setting.	option	-	disable
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Override the WTP profile split tunneling setting.		
	<i>disable</i>	Use the WTP profile split tunneling setting.		
override-wan-port-mode	Enable/disable overriding the wan-port-mode in the WTP profile.	option	-	disable
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Override the WTP profile wan-port-mode.		
	<i>disable</i>	Use the wan-port-mode in the WTP profile.		
region	Region name WTP is associated with.	string	Maximum length: 35	
region-x	Relative horizontal region coordinate (between 0 and 1).	string	Maximum length: 15	0
region-y	Relative vertical region coordinate (between 0 and 1).	string	Maximum length: 15	0
split-tunneling-acl-local-ap-subnet	Enable/disable automatically adding local subnetwork of FortiAP to split-tunneling ACL.	option	-	disable
	<b>Option</b> <b>Description</b>			
	<i>enable</i>	Enable automatically adding local subnetwork of FortiAP to split-tunneling ACL.		

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>disable</i>	Disable automatically adding local subnetwork of FortiAP to split-tunneling ACL.		
split-tunneling-acl-path	Split tunneling ACL path is local/tunnel.	option	-	local
	<b>Option</b>	<b>Description</b>		
	<i>tunnel</i>	Split tunneling ACL list traffic will be tunnel.		
	<i>local</i>	Split tunneling ACL list traffic will be local NATed.		
tun-mtu-downlink	The MTU of downlink CAPWAP tunnel.	integer	Minimum value: 576 Maximum value: 1500	0
tun-mtu-uplink	The maximum transmission unit.	integer	Minimum value: 576 Maximum value: 1500	0
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000
wan-port-mode	Enable/disable using the FortiAP WAN port as a LAN port.	option	-	wan-only
	<b>Option</b>	<b>Description</b>		
	<i>wan-lan</i>	Use the FortiAP WAN port as a LAN port.		
	<i>wan-only</i>	Do not use the WAN port as a LAN port.		
wtp-id	WTP ID.	string	Maximum length: 35	
wtp-profile	WTP profile name to apply to this WTP, AP or FortiAP.	string	Maximum length: 35	

## config lan

Parameter	Description	Type	Size	Default
port-mode	LAN port mode.	option	-	offline

Parameter	Description	Type	Size	Default
	<b>Option</b> <b>Description</b>			
	<i>offline</i>	Offline.		
	<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.		
	<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.		
	<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.		
port-ssid	Bridge LAN port to SSID.	string	Maximum length: 15	
port1-mode	LAN port 1 mode.	option	-	offline
	<b>Option</b> <b>Description</b>			
	<i>offline</i>	Offline.		
	<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.		
	<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.		
	<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.		
port1-ssid	Bridge LAN port 1 to SSID.	string	Maximum length: 15	
port2-mode	LAN port 2 mode.	option	-	offline
	<b>Option</b> <b>Description</b>			
	<i>offline</i>	Offline.		
	<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.		
	<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.		
	<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.		
port2-ssid	Bridge LAN port 2 to SSID.	string	Maximum length: 15	
port3-mode	LAN port 3 mode.	option	-	offline
	<b>Option</b> <b>Description</b>			
	<i>offline</i>	Offline.		
	<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.		
	<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.		
	<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.		

Parameter	Description	Type	Size	Default										
port3-ssid	Bridge LAN port 3 to SSID.	string	Maximum length: 15											
port4-mode	LAN port 4 mode.	option	-	offline										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>offline</td><td>Offline.</td></tr><tr><td>nat-to-wan</td><td>NAT WTP LAN port to WTP WAN port.</td></tr><tr><td>bridge-to-wan</td><td>Bridge WTP LAN port to WTP WAN port.</td></tr><tr><td>bridge-to-ssid</td><td>Bridge WTP LAN port to SSID.</td></tr></table>	Option	Description	offline	Offline.	nat-to-wan	NAT WTP LAN port to WTP WAN port.	bridge-to-wan	Bridge WTP LAN port to WTP WAN port.	bridge-to-ssid	Bridge WTP LAN port to SSID.			
	Option	Description												
	offline	Offline.												
	nat-to-wan	NAT WTP LAN port to WTP WAN port.												
	bridge-to-wan	Bridge WTP LAN port to WTP WAN port.												
	bridge-to-ssid	Bridge WTP LAN port to SSID.												
port4-ssid	Bridge LAN port 4 to SSID.	string	Maximum length: 15											
port5-mode	LAN port 5 mode.	option	-	offline										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>offline</td><td>Offline.</td></tr><tr><td>nat-to-wan</td><td>NAT WTP LAN port to WTP WAN port.</td></tr><tr><td>bridge-to-wan</td><td>Bridge WTP LAN port to WTP WAN port.</td></tr><tr><td>bridge-to-ssid</td><td>Bridge WTP LAN port to SSID.</td></tr></table>	Option	Description	offline	Offline.	nat-to-wan	NAT WTP LAN port to WTP WAN port.	bridge-to-wan	Bridge WTP LAN port to WTP WAN port.	bridge-to-ssid	Bridge WTP LAN port to SSID.			
	Option	Description												
	offline	Offline.												
	nat-to-wan	NAT WTP LAN port to WTP WAN port.												
	bridge-to-wan	Bridge WTP LAN port to WTP WAN port.												
	bridge-to-ssid	Bridge WTP LAN port to SSID.												
port5-ssid	Bridge LAN port 5 to SSID.	string	Maximum length: 15											
port6-mode	LAN port 6 mode.	option	-	offline										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>offline</td><td>Offline.</td></tr><tr><td>nat-to-wan</td><td>NAT WTP LAN port to WTP WAN port.</td></tr><tr><td>bridge-to-wan</td><td>Bridge WTP LAN port to WTP WAN port.</td></tr><tr><td>bridge-to-ssid</td><td>Bridge WTP LAN port to SSID.</td></tr></table>	Option	Description	offline	Offline.	nat-to-wan	NAT WTP LAN port to WTP WAN port.	bridge-to-wan	Bridge WTP LAN port to WTP WAN port.	bridge-to-ssid	Bridge WTP LAN port to SSID.			
	Option	Description												
	offline	Offline.												
	nat-to-wan	NAT WTP LAN port to WTP WAN port.												
	bridge-to-wan	Bridge WTP LAN port to WTP WAN port.												
	bridge-to-ssid	Bridge WTP LAN port to SSID.												
port6-ssid	Bridge LAN port 6 to SSID.	string	Maximum length: 15											
port7-mode	LAN port 7 mode.	option	-	offline										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>offline</td><td>Offline.</td></tr><tr><td>nat-to-wan</td><td>NAT WTP LAN port to WTP WAN port.</td></tr></table>	Option	Description	offline	Offline.	nat-to-wan	NAT WTP LAN port to WTP WAN port.							
	Option	Description												
	offline	Offline.												
nat-to-wan	NAT WTP LAN port to WTP WAN port.													



Parameter	Description	Type	Size	Default										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>bridge-to-wan</i></td><td>Bridge WTP LAN port to WTP WAN port.</td></tr><tr><td><i>bridge-to-ssid</i></td><td>Bridge WTP LAN port to SSID.</td></tr></table>	Option	Description	<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.	<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.							
	Option	Description												
	<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.												
<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.													
port7-ssid	Bridge LAN port 7 to SSID.	string	Maximum length: 15											
port8-mode	LAN port 8 mode.	option	-	offline										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>offline</i></td><td>Offline.</td></tr><tr><td><i>nat-to-wan</i></td><td>NAT WTP LAN port to WTP WAN port.</td></tr><tr><td><i>bridge-to-wan</i></td><td>Bridge WTP LAN port to WTP WAN port.</td></tr><tr><td><i>bridge-to-ssid</i></td><td>Bridge WTP LAN port to SSID.</td></tr></table>	Option	Description	<i>offline</i>	Offline.	<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.	<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.	<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.			
	Option	Description												
	<i>offline</i>	Offline.												
	<i>nat-to-wan</i>	NAT WTP LAN port to WTP WAN port.												
	<i>bridge-to-wan</i>	Bridge WTP LAN port to WTP WAN port.												
<i>bridge-to-ssid</i>	Bridge WTP LAN port to SSID.													
port8-ssid	Bridge LAN port 8 to SSID.	string	Maximum length: 15											
port-esl-mode	ESL port mode.	option	-	offline										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>offline</i></td><td>Offline.</td></tr><tr><td><i>nat-to-wan</i></td><td>NAT WTP ESL port to WTP WAN port.</td></tr><tr><td><i>bridge-to-wan</i></td><td>Bridge WTP ESL port to WTP WAN port.</td></tr><tr><td><i>bridge-to-ssid</i></td><td>Bridge WTP ESL port to SSID.</td></tr></table>	Option	Description	<i>offline</i>	Offline.	<i>nat-to-wan</i>	NAT WTP ESL port to WTP WAN port.	<i>bridge-to-wan</i>	Bridge WTP ESL port to WTP WAN port.	<i>bridge-to-ssid</i>	Bridge WTP ESL port to SSID.			
	Option	Description												
	<i>offline</i>	Offline.												
	<i>nat-to-wan</i>	NAT WTP ESL port to WTP WAN port.												
	<i>bridge-to-wan</i>	Bridge WTP ESL port to WTP WAN port.												
<i>bridge-to-ssid</i>	Bridge WTP ESL port to SSID.													
port-esl-ssid	Bridge ESL port to SSID.	string	Maximum length: 15											

### config radio-1

Parameter	Description	Type	Size	Default						
override-band	Enable to override the WTP profile band setting.	option	-	disable						
	<table><tr><th>Option</th><th>Description</th></tr><tr><td><i>enable</i></td><td>Override the WTP profile band setting.</td></tr><tr><td><i>disable</i></td><td>Use the WTP profile band setting.</td></tr></table>				Option	Description	<i>enable</i>	Override the WTP profile band setting.	<i>disable</i>	Use the WTP profile band setting.
	Option	Description								
	<i>enable</i>	Override the WTP profile band setting.								
	<i>disable</i>	Use the WTP profile band setting.								
band	WiFi band that Radio 1 operates on.	option	-							

Parameter	Description	Type	Size	Default																																															
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>802.11a</td><td>802.11a.</td></tr><tr><td>802.11b</td><td>802.11b.</td></tr><tr><td>802.11g</td><td>802.11g/b.</td></tr><tr><td>802.11n</td><td>802.11n/g/b at 2.4GHz.</td></tr><tr><td>802.11n-5G</td><td>802.11n/a at 5GHz.</td></tr><tr><td>802.11ac</td><td>802.11ac/n/a.</td></tr><tr><td>802.11ax-5G</td><td>802.11ax/ac/n/a at 5GHz.</td></tr><tr><td>802.11ax</td><td>802.11ax/n/g/b at 2.4GHz.</td></tr><tr><td>802.11ac-2G</td><td>802.11ac at 2.4GHz.</td></tr><tr><td>802.11ax-6G</td><td>802.11ax at 6GHz.</td></tr><tr><td>802.11n,g-only</td><td>802.11n/g at 2.4GHz.</td></tr><tr><td>802.11g-only</td><td>802.11g.</td></tr><tr><td>802.11n-only</td><td>802.11n at 2.4GHz.</td></tr><tr><td>802.11n-5G-only</td><td>802.11n at 5GHz.</td></tr><tr><td>802.11ac,n-only</td><td>802.11ac/n.</td></tr><tr><td>802.11ac-only</td><td>802.11ac.</td></tr><tr><td>802.11ax,ac-only</td><td>802.11ax/ac at 5GHz.</td></tr><tr><td>802.11ax,ac,n-only</td><td>802.11ax/ac/n at 5GHz.</td></tr><tr><td>802.11ax-5G-only</td><td>802.11ax at 5GHz.</td></tr><tr><td>802.11ax,n-only</td><td>802.11ax/n at 2.4GHz.</td></tr><tr><td>802.11ax,n,g-only</td><td>802.11ax/n/g at 2.4GHz.</td></tr><tr><td>802.11ax-only</td><td>802.11ax at 2.4GHz.</td></tr></table>	Option	Description	802.11a	802.11a.	802.11b	802.11b.	802.11g	802.11g/b.	802.11n	802.11n/g/b at 2.4GHz.	802.11n-5G	802.11n/a at 5GHz.	802.11ac	802.11ac/n/a.	802.11ax-5G	802.11ax/ac/n/a at 5GHz.	802.11ax	802.11ax/n/g/b at 2.4GHz.	802.11ac-2G	802.11ac at 2.4GHz.	802.11ax-6G	802.11ax at 6GHz.	802.11n,g-only	802.11n/g at 2.4GHz.	802.11g-only	802.11g.	802.11n-only	802.11n at 2.4GHz.	802.11n-5G-only	802.11n at 5GHz.	802.11ac,n-only	802.11ac/n.	802.11ac-only	802.11ac.	802.11ax,ac-only	802.11ax/ac at 5GHz.	802.11ax,ac,n-only	802.11ax/ac/n at 5GHz.	802.11ax-5G-only	802.11ax at 5GHz.	802.11ax,n-only	802.11ax/n at 2.4GHz.	802.11ax,n,g-only	802.11ax/n/g at 2.4GHz.	802.11ax-only	802.11ax at 2.4GHz.				
	Option	Description																																																	
	802.11a	802.11a.																																																	
	802.11b	802.11b.																																																	
	802.11g	802.11g/b.																																																	
	802.11n	802.11n/g/b at 2.4GHz.																																																	
	802.11n-5G	802.11n/a at 5GHz.																																																	
	802.11ac	802.11ac/n/a.																																																	
	802.11ax-5G	802.11ax/ac/n/a at 5GHz.																																																	
	802.11ax	802.11ax/n/g/b at 2.4GHz.																																																	
	802.11ac-2G	802.11ac at 2.4GHz.																																																	
	802.11ax-6G	802.11ax at 6GHz.																																																	
	802.11n,g-only	802.11n/g at 2.4GHz.																																																	
	802.11g-only	802.11g.																																																	
	802.11n-only	802.11n at 2.4GHz.																																																	
	802.11n-5G-only	802.11n at 5GHz.																																																	
	802.11ac,n-only	802.11ac/n.																																																	
	802.11ac-only	802.11ac.																																																	
	802.11ax,ac-only	802.11ax/ac at 5GHz.																																																	
	802.11ax,ac,n-only	802.11ax/ac/n at 5GHz.																																																	
	802.11ax-5G-only	802.11ax at 5GHz.																																																	
802.11ax,n-only	802.11ax/n at 2.4GHz.																																																		
802.11ax,n,g-only	802.11ax/n/g at 2.4GHz.																																																		
802.11ax-only	802.11ax at 2.4GHz.																																																		
override-txpower	Enable to override the WTP profile power level configuration.	option	-	disable																																															
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Override the WTP profile power level configuration.</td></tr><tr><td>disable</td><td>Use the WTP profile power level configuration.</td></tr></table>	Option	Description	enable	Override the WTP profile power level configuration.	disable	Use the WTP profile power level configuration.																																												
	Option	Description																																																	
	enable	Override the WTP profile power level configuration.																																																	
disable	Use the WTP profile power level configuration.																																																		
auto-power-level	Enable/disable automatic power-level adjustment to prevent co-channel interference.	option	-	disable																																															

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable automatic transmit power adjustment.		
	<i>disable</i>	Disable automatic transmit power adjustment.		
auto-power-high	The upper bound of automatic transmit power adjustment in dBm (the actual range of transmit power depends on the AP platform type).	integer	Minimum value: 0 Maximum value: 4294967295	17
auto-power-low	The lower bound of automatic transmit power adjustment in dBm (the actual range of transmit power depends on the AP platform type).	integer	Minimum value: 0 Maximum value: 4294967295	10
auto-power-target	Target of automatic transmit power adjustment in dBm.	string	Maximum length: 7	-70
power-mode	Set radio effective isotropic radiated power. This power takes into account both radio transmit power and antenna gain. Higher power level settings may be constrained by local regulatory requirements and AP capabilities.	option	-	percentage
	<b>Option</b>	<b>Description</b>		
	<i>dBm</i>	Set radio EIRP power in dBm.		
	<i>percentage</i>	Set radio EIRP power by percentage.		
power-level	Radio EIRP power level as a percentage of the maximum EIRP power.	integer	Minimum value: 0 Maximum value: 100	100
power-value	Radio EIRP power in dBm.	integer	Minimum value: 1 Maximum value: 33	27
override-vaps	Enable to override WTP profile Virtual Access Point (VAP) settings.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Override WTP profile VAP settings.		
	<i>disable</i>	Use WTP profile VAP settings.		

Parameter	Description	Type	Size	Default										
vap-all	Configure method for assigning SSIDs to this FortiAP.	option	-	tunnel										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>tunnel</td><td>Automatically select tunnel SSIDs.</td></tr><tr><td>bridge</td><td>Automatically select local-bridging SSIDs.</td></tr><tr><td>manual</td><td>Manually select SSIDs.</td></tr></table>	Option	Description	tunnel	Automatically select tunnel SSIDs.	bridge	Automatically select local-bridging SSIDs.	manual	Manually select SSIDs.					
Option	Description													
tunnel	Automatically select tunnel SSIDs.													
bridge	Automatically select local-bridging SSIDs.													
manual	Manually select SSIDs.													
vaps <name>	Manually selected list of Virtual Access Points (VAPs). Virtual Access Point (VAP) name.	string	Maximum length: 35											
override-channel	Enable to override WTP profile channel settings.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Override WTP profile channel settings.</td></tr><tr><td>disable</td><td>Use WTP profile channel settings.</td></tr></table>	Option	Description	enable	Override WTP profile channel settings.	disable	Use WTP profile channel settings.							
Option	Description													
enable	Override WTP profile channel settings.													
disable	Use WTP profile channel settings.													
channel <chan>	Selected list of wireless radio channels. Channel number.	string	Maximum length: 3											
drma-manual-mode	Radio mode to be used for DRMA manual mode.	option	-	ncf										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ap</td><td>Set the radio to AP mode.</td></tr><tr><td>monitor</td><td>Set the radio to monitor mode</td></tr><tr><td>ncf</td><td>Select and set the radio mode based on NCF score.</td></tr><tr><td>ncf-peek</td><td>Select the radio mode based on NCF score, but do not apply.</td></tr></table>	Option	Description	ap	Set the radio to AP mode.	monitor	Set the radio to monitor mode	ncf	Select and set the radio mode based on NCF score.	ncf-peek	Select the radio mode based on NCF score, but do not apply.			
Option	Description													
ap	Set the radio to AP mode.													
monitor	Set the radio to monitor mode													
ncf	Select and set the radio mode based on NCF score.													
ncf-peek	Select the radio mode based on NCF score, but do not apply.													

## config radio-2

Parameter	Description	Type	Size	Default
override-band	Enable to override the WTP profile band setting.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Override the WTP profile band setting.		
	<i>disable</i>	Use the WTP profile band setting.		
band	WiFi band that Radio 2 operates on.	option	-	

Parameter	Description	Type	Size	Default																																															
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>802.11a</td><td>802.11a.</td></tr><tr><td>802.11b</td><td>802.11b.</td></tr><tr><td>802.11g</td><td>802.11g/b.</td></tr><tr><td>802.11n</td><td>802.11n/g/b at 2.4GHz.</td></tr><tr><td>802.11n-5G</td><td>802.11n/a at 5GHz.</td></tr><tr><td>802.11ac</td><td>802.11ac/n/a.</td></tr><tr><td>802.11ax-5G</td><td>802.11ax/ac/n/a at 5GHz.</td></tr><tr><td>802.11ax</td><td>802.11ax/n/g/b at 2.4GHz.</td></tr><tr><td>802.11ac-2G</td><td>802.11ac at 2.4GHz.</td></tr><tr><td>802.11ax-6G</td><td>802.11ax at 6GHz.</td></tr><tr><td>802.11n,g-only</td><td>802.11n/g at 2.4GHz.</td></tr><tr><td>802.11g-only</td><td>802.11g.</td></tr><tr><td>802.11n-only</td><td>802.11n at 2.4GHz.</td></tr><tr><td>802.11n-5G-only</td><td>802.11n at 5GHz.</td></tr><tr><td>802.11ac,n-only</td><td>802.11ac/n.</td></tr><tr><td>802.11ac-only</td><td>802.11ac.</td></tr><tr><td>802.11ax,ac-only</td><td>802.11ax/ac at 5GHz.</td></tr><tr><td>802.11ax,ac,n-only</td><td>802.11ax/ac/n at 5GHz.</td></tr><tr><td>802.11ax-5G-only</td><td>802.11ax at 5GHz.</td></tr><tr><td>802.11ax,n-only</td><td>802.11ax/n at 2.4GHz.</td></tr><tr><td>802.11ax,n,g-only</td><td>802.11ax/n/g at 2.4GHz.</td></tr><tr><td>802.11ax-only</td><td>802.11ax at 2.4GHz.</td></tr></table>	Option	Description	802.11a	802.11a.	802.11b	802.11b.	802.11g	802.11g/b.	802.11n	802.11n/g/b at 2.4GHz.	802.11n-5G	802.11n/a at 5GHz.	802.11ac	802.11ac/n/a.	802.11ax-5G	802.11ax/ac/n/a at 5GHz.	802.11ax	802.11ax/n/g/b at 2.4GHz.	802.11ac-2G	802.11ac at 2.4GHz.	802.11ax-6G	802.11ax at 6GHz.	802.11n,g-only	802.11n/g at 2.4GHz.	802.11g-only	802.11g.	802.11n-only	802.11n at 2.4GHz.	802.11n-5G-only	802.11n at 5GHz.	802.11ac,n-only	802.11ac/n.	802.11ac-only	802.11ac.	802.11ax,ac-only	802.11ax/ac at 5GHz.	802.11ax,ac,n-only	802.11ax/ac/n at 5GHz.	802.11ax-5G-only	802.11ax at 5GHz.	802.11ax,n-only	802.11ax/n at 2.4GHz.	802.11ax,n,g-only	802.11ax/n/g at 2.4GHz.	802.11ax-only	802.11ax at 2.4GHz.				
	Option	Description																																																	
	802.11a	802.11a.																																																	
	802.11b	802.11b.																																																	
	802.11g	802.11g/b.																																																	
	802.11n	802.11n/g/b at 2.4GHz.																																																	
	802.11n-5G	802.11n/a at 5GHz.																																																	
	802.11ac	802.11ac/n/a.																																																	
	802.11ax-5G	802.11ax/ac/n/a at 5GHz.																																																	
	802.11ax	802.11ax/n/g/b at 2.4GHz.																																																	
	802.11ac-2G	802.11ac at 2.4GHz.																																																	
	802.11ax-6G	802.11ax at 6GHz.																																																	
	802.11n,g-only	802.11n/g at 2.4GHz.																																																	
	802.11g-only	802.11g.																																																	
	802.11n-only	802.11n at 2.4GHz.																																																	
	802.11n-5G-only	802.11n at 5GHz.																																																	
	802.11ac,n-only	802.11ac/n.																																																	
	802.11ac-only	802.11ac.																																																	
	802.11ax,ac-only	802.11ax/ac at 5GHz.																																																	
	802.11ax,ac,n-only	802.11ax/ac/n at 5GHz.																																																	
	802.11ax-5G-only	802.11ax at 5GHz.																																																	
802.11ax,n-only	802.11ax/n at 2.4GHz.																																																		
802.11ax,n,g-only	802.11ax/n/g at 2.4GHz.																																																		
802.11ax-only	802.11ax at 2.4GHz.																																																		
override-txpower	Enable to override the WTP profile power level configuration.	option	-	disable																																															
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Override the WTP profile power level configuration.</td></tr><tr><td>disable</td><td>Use the WTP profile power level configuration.</td></tr></table>	Option	Description	enable	Override the WTP profile power level configuration.	disable	Use the WTP profile power level configuration.																																												
	Option	Description																																																	
	enable	Override the WTP profile power level configuration.																																																	
disable	Use the WTP profile power level configuration.																																																		
auto-power-level	Enable/disable automatic power-level adjustment to prevent co-channel interference.	option	-	disable																																															

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable automatic transmit power adjustment.		
	<i>disable</i>	Disable automatic transmit power adjustment.		
auto-power-high	The upper bound of automatic transmit power adjustment in dBm (the actual range of transmit power depends on the AP platform type).	integer	Minimum value: 0 Maximum value: 4294967295	17
auto-power-low	The lower bound of automatic transmit power adjustment in dBm (the actual range of transmit power depends on the AP platform type).	integer	Minimum value: 0 Maximum value: 4294967295	10
auto-power-target	Target of automatic transmit power adjustment in dBm.	string	Maximum length: 7	-70
power-mode	Set radio effective isotropic radiated power. This power takes into account both radio transmit power and antenna gain. Higher power level settings may be constrained by local regulatory requirements and AP capabilities.	option	-	percentage
	<b>Option</b>	<b>Description</b>		
	<i>dBm</i>	Set radio EIRP power in dBm.		
	<i>percentage</i>	Set radio EIRP power by percentage.		
power-level	Radio EIRP power level as a percentage of the maximum EIRP power.	integer	Minimum value: 0 Maximum value: 100	100
power-value	Radio EIRP power in dBm.	integer	Minimum value: 1 Maximum value: 33	27
override-vaps	Enable to override WTP profile Virtual Access Point (VAP) settings.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Override WTP profile VAP settings.		
	<i>disable</i>	Use WTP profile VAP settings.		

Parameter	Description	Type	Size	Default
vap-all	Configure method for assigning SSIDs to this FortiAP.	option	-	tunnel
	<b>Option</b>	<b>Description</b>		
	<i>tunnel</i>	Automatically select tunnel SSIDs.		
	<i>bridge</i>	Automatically select local-bridging SSIDs.		
	<i>manual</i>	Manually select SSIDs.		
vaps <name>	Manually selected list of Virtual Access Points (VAPs). Virtual Access Point (VAP) name.	string	Maximum length: 35	
override-channel	Enable to override WTP profile channel settings.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Override WTP profile channel settings.		
	<i>disable</i>	Use WTP profile channel settings.		
channel <chan>	Selected list of wireless radio channels. Channel number.	string	Maximum length: 3	
drma-manual-mode	Radio mode to be used for DRMA manual mode.	option	-	ncf
	<b>Option</b>	<b>Description</b>		
	<i>ap</i>	Set the radio to AP mode.		
	<i>monitor</i>	Set the radio to monitor mode		
	<i>ncf</i>	Select and set the radio mode based on NCF score.		
	<i>ncf-peek</i>	Select the radio mode based on NCF score, but do not apply.		

### config radio-3

Parameter	Description	Type	Size	Default
override-band	Enable to override the WTP profile band setting.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Override the WTP profile band setting.		
	<i>disable</i>	Use the WTP profile band setting.		
band	WiFi band that Radio 3 operates on.	option	-	

Parameter	Description	Type	Size	Default																																															
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>802.11a</td><td>802.11a.</td></tr><tr><td>802.11b</td><td>802.11b.</td></tr><tr><td>802.11g</td><td>802.11g/b.</td></tr><tr><td>802.11n</td><td>802.11n/g/b at 2.4GHz.</td></tr><tr><td>802.11n-5G</td><td>802.11n/a at 5GHz.</td></tr><tr><td>802.11ac</td><td>802.11ac/n/a.</td></tr><tr><td>802.11ax-5G</td><td>802.11ax/ac/n/a at 5GHz.</td></tr><tr><td>802.11ax</td><td>802.11ax/n/g/b at 2.4GHz.</td></tr><tr><td>802.11ac-2G</td><td>802.11ac at 2.4GHz.</td></tr><tr><td>802.11ax-6G</td><td>802.11ax at 6GHz.</td></tr><tr><td>802.11n,g-only</td><td>802.11n/g at 2.4GHz.</td></tr><tr><td>802.11g-only</td><td>802.11g.</td></tr><tr><td>802.11n-only</td><td>802.11n at 2.4GHz.</td></tr><tr><td>802.11n-5G-only</td><td>802.11n at 5GHz.</td></tr><tr><td>802.11ac,n-only</td><td>802.11ac/n.</td></tr><tr><td>802.11ac-only</td><td>802.11ac.</td></tr><tr><td>802.11ax,ac-only</td><td>802.11ax/ac at 5GHz.</td></tr><tr><td>802.11ax,ac,n-only</td><td>802.11ax/ac/n at 5GHz.</td></tr><tr><td>802.11ax-5G-only</td><td>802.11ax at 5GHz.</td></tr><tr><td>802.11ax,n-only</td><td>802.11ax/n at 2.4GHz.</td></tr><tr><td>802.11ax,n,g-only</td><td>802.11ax/n/g at 2.4GHz.</td></tr><tr><td>802.11ax-only</td><td>802.11ax at 2.4GHz.</td></tr></table>	Option	Description	802.11a	802.11a.	802.11b	802.11b.	802.11g	802.11g/b.	802.11n	802.11n/g/b at 2.4GHz.	802.11n-5G	802.11n/a at 5GHz.	802.11ac	802.11ac/n/a.	802.11ax-5G	802.11ax/ac/n/a at 5GHz.	802.11ax	802.11ax/n/g/b at 2.4GHz.	802.11ac-2G	802.11ac at 2.4GHz.	802.11ax-6G	802.11ax at 6GHz.	802.11n,g-only	802.11n/g at 2.4GHz.	802.11g-only	802.11g.	802.11n-only	802.11n at 2.4GHz.	802.11n-5G-only	802.11n at 5GHz.	802.11ac,n-only	802.11ac/n.	802.11ac-only	802.11ac.	802.11ax,ac-only	802.11ax/ac at 5GHz.	802.11ax,ac,n-only	802.11ax/ac/n at 5GHz.	802.11ax-5G-only	802.11ax at 5GHz.	802.11ax,n-only	802.11ax/n at 2.4GHz.	802.11ax,n,g-only	802.11ax/n/g at 2.4GHz.	802.11ax-only	802.11ax at 2.4GHz.				
	Option	Description																																																	
	802.11a	802.11a.																																																	
	802.11b	802.11b.																																																	
	802.11g	802.11g/b.																																																	
	802.11n	802.11n/g/b at 2.4GHz.																																																	
	802.11n-5G	802.11n/a at 5GHz.																																																	
	802.11ac	802.11ac/n/a.																																																	
	802.11ax-5G	802.11ax/ac/n/a at 5GHz.																																																	
	802.11ax	802.11ax/n/g/b at 2.4GHz.																																																	
	802.11ac-2G	802.11ac at 2.4GHz.																																																	
	802.11ax-6G	802.11ax at 6GHz.																																																	
	802.11n,g-only	802.11n/g at 2.4GHz.																																																	
	802.11g-only	802.11g.																																																	
	802.11n-only	802.11n at 2.4GHz.																																																	
	802.11n-5G-only	802.11n at 5GHz.																																																	
	802.11ac,n-only	802.11ac/n.																																																	
	802.11ac-only	802.11ac.																																																	
	802.11ax,ac-only	802.11ax/ac at 5GHz.																																																	
	802.11ax,ac,n-only	802.11ax/ac/n at 5GHz.																																																	
	802.11ax-5G-only	802.11ax at 5GHz.																																																	
802.11ax,n-only	802.11ax/n at 2.4GHz.																																																		
802.11ax,n,g-only	802.11ax/n/g at 2.4GHz.																																																		
802.11ax-only	802.11ax at 2.4GHz.																																																		
override-txpower	Enable to override the WTP profile power level configuration.	option	-	disable																																															
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Override the WTP profile power level configuration.</td></tr><tr><td>disable</td><td>Use the WTP profile power level configuration.</td></tr></table>	Option	Description	enable	Override the WTP profile power level configuration.	disable	Use the WTP profile power level configuration.																																												
	Option	Description																																																	
	enable	Override the WTP profile power level configuration.																																																	
disable	Use the WTP profile power level configuration.																																																		
auto-power-level	Enable/disable automatic power-level adjustment to prevent co-channel interference.	option	-	disable																																															



Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable automatic transmit power adjustment.		
	<i>disable</i>	Disable automatic transmit power adjustment.		
auto-power-high	The upper bound of automatic transmit power adjustment in dBm (the actual range of transmit power depends on the AP platform type).	integer	Minimum value: 0 Maximum value: 4294967295	17
auto-power-low	The lower bound of automatic transmit power adjustment in dBm (the actual range of transmit power depends on the AP platform type).	integer	Minimum value: 0 Maximum value: 4294967295	10
auto-power-target	Target of automatic transmit power adjustment in dBm.	string	Maximum length: 7	-70
power-mode	Set radio effective isotropic radiated power. This power takes into account both radio transmit power and antenna gain. Higher power level settings may be constrained by local regulatory requirements and AP capabilities.	option	-	percentage
	<b>Option</b>	<b>Description</b>		
	<i>dBm</i>	Set radio EIRP power in dBm.		
	<i>percentage</i>	Set radio EIRP power by percentage.		
power-level	Radio EIRP power level as a percentage of the maximum EIRP power.	integer	Minimum value: 0 Maximum value: 100	100
power-value	Radio EIRP power in dBm.	integer	Minimum value: 1 Maximum value: 33	27
override-vaps	Enable to override WTP profile Virtual Access Point (VAP) settings.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Override WTP profile VAP settings.		
	<i>disable</i>	Use WTP profile VAP settings.		

Parameter	Description	Type	Size	Default										
vap-all	Configure method for assigning SSIDs to this FortiAP.	option	-	tunnel										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>tunnel</td><td>Automatically select tunnel SSIDs.</td></tr><tr><td>bridge</td><td>Automatically select local-bridging SSIDs.</td></tr><tr><td>manual</td><td>Manually select SSIDs.</td></tr></table>	Option	Description	tunnel	Automatically select tunnel SSIDs.	bridge	Automatically select local-bridging SSIDs.	manual	Manually select SSIDs.					
Option	Description													
tunnel	Automatically select tunnel SSIDs.													
bridge	Automatically select local-bridging SSIDs.													
manual	Manually select SSIDs.													
vaps <name>	Manually selected list of Virtual Access Points (VAPs). Virtual Access Point (VAP) name.	string	Maximum length: 35											
override-channel	Enable to override WTP profile channel settings.	option	-	disable										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Override WTP profile channel settings.</td></tr><tr><td>disable</td><td>Use WTP profile channel settings.</td></tr></table>	Option	Description	enable	Override WTP profile channel settings.	disable	Use WTP profile channel settings.							
Option	Description													
enable	Override WTP profile channel settings.													
disable	Use WTP profile channel settings.													
channel <chan>	Selected list of wireless radio channels. Channel number.	string	Maximum length: 3											
drma-manual-mode	Radio mode to be used for DRMA manual mode.	option	-	ncf										
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>ap</td><td>Set the radio to AP mode.</td></tr><tr><td>monitor</td><td>Set the radio to monitor mode</td></tr><tr><td>ncf</td><td>Select and set the radio mode based on NCF score.</td></tr><tr><td>ncf-peek</td><td>Select the radio mode based on NCF score, but do not apply.</td></tr></table>	Option	Description	ap	Set the radio to AP mode.	monitor	Set the radio to monitor mode	ncf	Select and set the radio mode based on NCF score.	ncf-peek	Select the radio mode based on NCF score, but do not apply.			
Option	Description													
ap	Set the radio to AP mode.													
monitor	Set the radio to monitor mode													
ncf	Select and set the radio mode based on NCF score.													
ncf-peek	Select the radio mode based on NCF score, but do not apply.													

## config radio-4

Parameter	Description	Type	Size	Default
override-band	Enable to override the WTP profile band setting.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Override the WTP profile band setting.		
	<i>disable</i>	Use the WTP profile band setting.		
band	WiFi band that Radio 4 operates on.	option	-	

Parameter	Description	Type	Size	Default																																															
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>802.11a</td><td>802.11a.</td></tr><tr><td>802.11b</td><td>802.11b.</td></tr><tr><td>802.11g</td><td>802.11g/b.</td></tr><tr><td>802.11n</td><td>802.11n/g/b at 2.4GHz.</td></tr><tr><td>802.11n-5G</td><td>802.11n/a at 5GHz.</td></tr><tr><td>802.11ac</td><td>802.11ac/n/a.</td></tr><tr><td>802.11ax-5G</td><td>802.11ax/ac/n/a at 5GHz.</td></tr><tr><td>802.11ax</td><td>802.11ax/n/g/b at 2.4GHz.</td></tr><tr><td>802.11ac-2G</td><td>802.11ac at 2.4GHz.</td></tr><tr><td>802.11ax-6G</td><td>802.11ax at 6GHz.</td></tr><tr><td>802.11n,g-only</td><td>802.11n/g at 2.4GHz.</td></tr><tr><td>802.11g-only</td><td>802.11g.</td></tr><tr><td>802.11n-only</td><td>802.11n at 2.4GHz.</td></tr><tr><td>802.11n-5G-only</td><td>802.11n at 5GHz.</td></tr><tr><td>802.11ac,n-only</td><td>802.11ac/n.</td></tr><tr><td>802.11ac-only</td><td>802.11ac.</td></tr><tr><td>802.11ax,ac-only</td><td>802.11ax/ac at 5GHz.</td></tr><tr><td>802.11ax,ac,n-only</td><td>802.11ax/ac/n at 5GHz.</td></tr><tr><td>802.11ax-5G-only</td><td>802.11ax at 5GHz.</td></tr><tr><td>802.11ax,n-only</td><td>802.11ax/n at 2.4GHz.</td></tr><tr><td>802.11ax,n,g-only</td><td>802.11ax/n/g at 2.4GHz.</td></tr><tr><td>802.11ax-only</td><td>802.11ax at 2.4GHz.</td></tr></table>	Option	Description	802.11a	802.11a.	802.11b	802.11b.	802.11g	802.11g/b.	802.11n	802.11n/g/b at 2.4GHz.	802.11n-5G	802.11n/a at 5GHz.	802.11ac	802.11ac/n/a.	802.11ax-5G	802.11ax/ac/n/a at 5GHz.	802.11ax	802.11ax/n/g/b at 2.4GHz.	802.11ac-2G	802.11ac at 2.4GHz.	802.11ax-6G	802.11ax at 6GHz.	802.11n,g-only	802.11n/g at 2.4GHz.	802.11g-only	802.11g.	802.11n-only	802.11n at 2.4GHz.	802.11n-5G-only	802.11n at 5GHz.	802.11ac,n-only	802.11ac/n.	802.11ac-only	802.11ac.	802.11ax,ac-only	802.11ax/ac at 5GHz.	802.11ax,ac,n-only	802.11ax/ac/n at 5GHz.	802.11ax-5G-only	802.11ax at 5GHz.	802.11ax,n-only	802.11ax/n at 2.4GHz.	802.11ax,n,g-only	802.11ax/n/g at 2.4GHz.	802.11ax-only	802.11ax at 2.4GHz.				
	Option	Description																																																	
	802.11a	802.11a.																																																	
	802.11b	802.11b.																																																	
	802.11g	802.11g/b.																																																	
	802.11n	802.11n/g/b at 2.4GHz.																																																	
	802.11n-5G	802.11n/a at 5GHz.																																																	
	802.11ac	802.11ac/n/a.																																																	
	802.11ax-5G	802.11ax/ac/n/a at 5GHz.																																																	
	802.11ax	802.11ax/n/g/b at 2.4GHz.																																																	
	802.11ac-2G	802.11ac at 2.4GHz.																																																	
	802.11ax-6G	802.11ax at 6GHz.																																																	
	802.11n,g-only	802.11n/g at 2.4GHz.																																																	
	802.11g-only	802.11g.																																																	
	802.11n-only	802.11n at 2.4GHz.																																																	
	802.11n-5G-only	802.11n at 5GHz.																																																	
	802.11ac,n-only	802.11ac/n.																																																	
	802.11ac-only	802.11ac.																																																	
	802.11ax,ac-only	802.11ax/ac at 5GHz.																																																	
	802.11ax,ac,n-only	802.11ax/ac/n at 5GHz.																																																	
	802.11ax-5G-only	802.11ax at 5GHz.																																																	
802.11ax,n-only	802.11ax/n at 2.4GHz.																																																		
802.11ax,n,g-only	802.11ax/n/g at 2.4GHz.																																																		
802.11ax-only	802.11ax at 2.4GHz.																																																		
override-txpower	Enable to override the WTP profile power level configuration.	option	-	disable																																															
	<table><tr><th>Option</th><th>Description</th></tr><tr><td>enable</td><td>Override the WTP profile power level configuration.</td></tr><tr><td>disable</td><td>Use the WTP profile power level configuration.</td></tr></table>	Option	Description	enable	Override the WTP profile power level configuration.	disable	Use the WTP profile power level configuration.																																												
	Option	Description																																																	
	enable	Override the WTP profile power level configuration.																																																	
disable	Use the WTP profile power level configuration.																																																		
auto-power-level	Enable/disable automatic power-level adjustment to prevent co-channel interference.	option	-	disable																																															

Parameter	Description	Type	Size	Default
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Enable automatic transmit power adjustment.		
	<i>disable</i>	Disable automatic transmit power adjustment.		
auto-power-high	The upper bound of automatic transmit power adjustment in dBm (the actual range of transmit power depends on the AP platform type).	integer	Minimum value: 0 Maximum value: 4294967295	17
auto-power-low	The lower bound of automatic transmit power adjustment in dBm (the actual range of transmit power depends on the AP platform type).	integer	Minimum value: 0 Maximum value: 4294967295	10
auto-power-target	Target of automatic transmit power adjustment in dBm.	string	Maximum length: 7	-70
power-mode	Set radio effective isotropic radiated power. This power takes into account both radio transmit power and antenna gain. Higher power level settings may be constrained by local regulatory requirements and AP capabilities.	option	-	percentage
	<b>Option</b>	<b>Description</b>		
	<i>dBm</i>	Set radio EIRP power in dBm.		
	<i>percentage</i>	Set radio EIRP power by percentage.		
power-level	Radio EIRP power level as a percentage of the maximum EIRP power.	integer	Minimum value: 0 Maximum value: 100	100
power-value	Radio EIRP power in dBm.	integer	Minimum value: 1 Maximum value: 33	27
override-vaps	Enable to override WTP profile Virtual Access Point (VAP) settings.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Override WTP profile VAP settings.		
	<i>disable</i>	Use WTP profile VAP settings.		

Parameter	Description	Type	Size	Default
vap-all	Configure method for assigning SSIDs to this FortiAP.	option	-	tunnel
	<b>Option</b>	<b>Description</b>		
	<i>tunnel</i>	Automatically select tunnel SSIDs.		
	<i>bridge</i>	Automatically select local-bridging SSIDs.		
	<i>manual</i>	Manually select SSIDs.		
vaps <name>	Manually selected list of Virtual Access Points (VAPs). Virtual Access Point (VAP) name.	string	Maximum length: 35	
override-channel	Enable to override WTP profile channel settings.	option	-	disable
	<b>Option</b>	<b>Description</b>		
	<i>enable</i>	Override WTP profile channel settings.		
	<i>disable</i>	Use WTP profile channel settings.		
channel <chan>	Selected list of wireless radio channels. Channel number.	string	Maximum length: 3	
drma-manual-mode	Radio mode to be used for DRMA manual mode.	option	-	ncf
	<b>Option</b>	<b>Description</b>		
	<i>ap</i>	Set the radio to AP mode.		
	<i>monitor</i>	Set the radio to monitor mode		
	<i>ncf</i>	Select and set the radio mode based on NCF score.		
	<i>ncf-peek</i>	Select the radio mode based on NCF score, but do not apply.		

## config split-tunneling-acl

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
dest-ip	Destination IP and mask for the split-tunneling subnet.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0



[www.fortinet.com](http://www.fortinet.com)

Copyright© 2023 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.